



FortiManager - CLI Reference

VERSION 5.0.12

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



June 14, 2016

FortiManager 5.0.12 CLI Reference

02-5012-183470-20160614

TABLE OF CONTENTS

Change Log	12
Introduction	13
About the FortiManager system	13
FortiManager feature set	13
FortiAnalyzer feature set	13
GUI	13
FortiManager system product life cycle	14
FortiManager documentation	14
What's New in FortiManager version 5.0	15
FortiManager version 5.0.12	15
FortiManager version 5.0.11	15
FortiManager version 5.0.10	15
FortiManager version 5.0.9	16
FortiManager version 5.0.8	17
FortiManager version 5.0.7	17
FortiManager version 5.0.6	20
FortiManager version 5.0.5	21
FortiManager version 5.0.4	21
FortiManager version 5.0.3	22
Using the Command Line Interface	27
CLI command syntax	27
Connecting to the CLI	28
Connecting to the FortiManager console	28
Setting administrative access on an interface	29
Connecting to the FortiManager CLI using SSH	29
Connecting to the FortiManager CLI using the GUI	30
CLI objects	30
CLI command branches	30
config branch	30
get branch	32
show branch	34
execute branch	35
diagnose branch	35
Example command sequences	36

CLI basics	36
Command help	36
Command tree	37
Command completion	37
Recalling commands	37
Editing commands	37
Line continuation	38
Command abbreviation	38
Environment variables	38
Encrypted password support	39
Entering spaces in strings	39
Entering quotation marks in strings	39
Entering a question mark (?) in a string	39
International characters	40
Special characters	40
IP address formats	40
Editing the configuration file	40
Changing the baud rate	40
Debug log levels	41
Administrative Domains	42
ADOMs overview	42
Configuring ADOMs	43
Concurrent ADOM Access	44
system	45
admin	45
admin group	45
admin ldap	45
admin profile	47
admin radius	53
admin setting	54
admin tacacs	58
admin user	59
alert-console	66
alert-event	67
alertemail	69
auto-delete	70
backup all-settings	71
certificate	73
certificate ca	73
certificate crl	74
certificate local	74
certificate oftp	75

certificate ssh	75
dm	76
dns	78
fips	79
global	79
ha	85
General FortiManager HA configuration steps	87
interface	88
locallog	90
locallog disk setting	90
locallog filter	93
locallog fortianalyzer setting	95
locallog memory setting	96
locallog syslogd (syslogd2, syslogd3) setting	97
log	99
log alert	99
log fortianalyzer	99
log settings	100
mail	103
metadata	104
ntp	104
password-policy	105
report	106
report auto-cache	106
report est-browse-time	107
report group	107
report setting	108
route	109
route6	109
snmp	110
snmp community	110
snmp sysinfo	113
snmp user	114
sql	116
syslog	119
fmupdate	121
analyzer virusreport	121
av-ips	121
av-ips advanced-log	121
av-ips fct server-override	122
av-ips fgt server-override	123
av-ips push-override	123

av-ips push-override-to-client	124
av-ips update-schedule	125
av-ips web-proxy	126
custom-url-list	127
device-version	127
disk-quota	129
fct-services	129
fds-setting	129
multilayer	130
publicnetwork	130
server-access-priorities	131
config private-server	131
server-override-status	132
service	132
support-pre-fgt43	133
web-spam	134
web-spam fct server-override	134
web-spam fgd-log	134
web-spam fgd-setting	135
web-spam fgt server-override	137
web-spam fsa server-override	138
web-spam poll-frequency	138
web-spam web-proxy	139
execute	140
add-vm-license	140
backup	140
bootimage	142
certificate	142
certificate ca	142
certificate local	143
chassis	144
console baudrate	145
date	145
device	146
dmserver	146
dmserver delrev	146
dmserver revlist	146
dmserver showconfig	147
dmserver showdev	147
dmserver showrev	147
factory-license	147
fgfm reclaim-dev-tunnel	148

fmpolicy	148
fmpolicy check-upgrade-object	148
fmpolicy copy-adom-object	149
fmpolicy install-config	149
fmpolicy print-adom-database	150
fmpolicy print-adom-object	150
fmpolicy print-adom-package	150
fmpolicy print-device-database	151
fmpolicy print-device-object	151
fmpolicy print-prov-templates	152
fmprofile	152
fmprofile copy-to-device	152
fmprofile export-profile	153
fmprofile import-from-device	153
fmprofile import-profile	153
fmprofile list-profiles	153
fmscript	154
fmscript clean-sched	154
fmscript delete	154
fmscript import	154
fmscript list	155
fmscript run	156
fmscript showlog	156
fmupdate	157
fmupdate {ftp scp tftp} import	157
fmupdate {ftp scp tftp} export	157
format	158
log	159
log device disk_quota	159
log device permissions	159
log dlp-files clear	160
log import	160
log ips-pkt clear	161
log quarantine-files clear	161
log-integrity	161
lvm	161
ping	162
ping6	163
raid	163
reboot	163
remove	164
reset	164

reset-sqllog-transfer	164
restore	165
shutdown	166
sql-local	167
sql-local rebuild-db	167
sql-local remove-db	167
sql-local remove-logtype	167
sql-query-dataset	168
sql-query-generic	168
sql-report	169
sql-report hcache-check	169
sql-report import-lang	169
sql-report list	170
sql-report list-lang	170
sql-report list-schedule	170
sql-report run	170
sql-report view	171
ssh	171
ssh-known-hosts	172
time	172
top	173
traceroute	174
traceroute6	174
diagnose	176
auto-delete	176
cdb check	177
debug	177
debug application	177
debug cli	180
debug console	181
debug crashlog	181
debug disable	181
debug dpm	181
debug enable	182
debug info	182
debug reset	183
debug service	183
debug sysinfo	183
debug sysinfo-log	184
debug sysinfo-log-backup	184
debug sysinfo-log-list	185
debug timestamp	185

debug vminfo	185
dlp-archives	186
dvm	186
dvm adom	186
dvm capability	186
dvm chassis	187
dvm check-integrity	187
dvm debug	187
dvm device	188
dvm device-tree-update	188
dvm extender	188
dvm group	189
dvm lock	189
dvm proc	189
dvm supported-platforms	190
dvm task	190
dvm transaction-flag	191
fgfm	191
fmnetwork	191
fmnetwork arp	191
fmnetwork interface	192
fmnetwork netstat	193
fmupdate	193
fortilogd	198
fwmanager	199
ha	200
hardware	201
log	203
log device	203
pm2	203
report	203
sniffer	204
sql	208
system	209
system admin-session	210
system disk	210
system export	211
system flash	212
system fsck	212
system geoip	212
system ntp	213
system print	213

system process	214
system raid	215
system route	215
system route6	216
system server	216
test	216
test application	216
test connection	217
test deploymanager	217
test policy-check	218
test search	218
test sftp	218
upload	219
upload clear	219
upload force-retry	219
upload status	219
vpn	219
get	221
fmupdate analyzer	221
fmupdate av-ips	221
fmupdate custom-url-list	222
fmupdate device-version	222
fmupdate disk-quota	222
fmupdate fct-services	222
fmupdate fds-setting	223
fmupdate multilayer	223
fmupdate publicnetwork	223
fmupdate server-access-priorities	223
fmupdate server-override-status	224
fmupdate service	224
fmupdate support-pre-ftg43	224
fmupdate web-spam	224
system admin	225
system alert-console	226
system alert-event	226
system alertemail	226
system auto-delete	227
system backup	227
system certificate	227
system dm	228
system dns	228
system fips	228

system global	228
system ha	229
system interface	230
system locallog	230
system log	231
system mail	231
system metadata	231
system ntp	232
system password-policy	232
system performance	232
system report	233
system route	233
system route6	233
system snmp	233
system sql	234
system status	235
system syslog	236
show	237

Change Log

Date	Change Description
2012-11-16	Initial release.
2013-04-02	Updated for FortiManager 5.0.2. Changed all instances of <code>fmsystem</code> and <code>fasystem</code> to <code>system</code> .
2013-07-19	Updated for FortiManager 5.0.3.
2013-09-13	Updated for FortiManager 5.0.4.
2013-11-12	Updated for FortiManager 5.0.5.
2014-02-05	Updated for FortiManager 5.0.6.
2014-07-02	Updated for FortiManager 5.0.7.
2014-10-07	Updated for FortiManager 5.0.8.
2014-10-22	Updated for FortiManager 5.0.9.
2015-01-29	Updated for FortiManager 5.0.10.
2015-06-18	Updated for FortiManager 5.0.11.
2016-07-14	Updated for FortiManager 5.0.12

Introduction

FortiManager centralized management appliances deliver the essential tools needed to effectively manage your Fortinet-based security infrastructure.

About the FortiManager system

The FortiManager system is a security-hardened appliance with simplified installation, and improved system reliability and security. You can install a second peer FortiManager system for database backups.

The FortiManager system manages communication between the managed devices and the FortiManager GUI.

The FortiManager system stores and manages all managed devices' configurations.

It can also act as a local FortiGuard Distribution Server (FDS) for the managed devices to download virus and attack signatures, and to use the web filtering and email filtering service. This will reduce network delay and usage, compared with the managed devices' connection to an FDS over the Internet.

FortiManager feature set

The FortiManager feature set includes the following modules:

- Device Manager
- Policy & Objects
- FortiGuard
- System Settings

FortiAnalyzer feature set

The FortiAnalyzer feature set can be enabled in FortiManager. The FortiAnalyzer feature set includes the following modules:

- FortiView
- Event Management
- Reports

GUI

You can use the FortiManager GUI to configure the managed devices and to view the device configuration, device status, system health, and logs. The FortiManager GUI supports role-based administration. Permissions and device access can be set individually for each manager account added to the FortiManager GUI.

Administrators with read and write access can view the configuration, health status, and logs, and can change the configurations of the devices assigned to them. The FortiManager GUI also allows these users to remotely upgrade device firmware, and virus and attack definitions.

Administrators with read only access can view the configuration, device status, system health, and logs of the devices assigned to them.

FortiManager system product life cycle

The FortiManager system allows you to manage devices through their entire product life cycle:

Deployment	Complete device configuration after initial installation.
Monitoring	Drill down device status and health.
Maintenance	Continuous, incremental configuration and updates.
Updates	Updates of virus definitions, attack definitions, web filtering service, email filter service, and firmware images.

FortiManager documentation

The following FortiManager product documentation is available:

- *FortiManager Administration Guide*

This document describes how to set up the FortiManager system and use it to manage supported Fortinet units. It includes information on how to configure multiple Fortinet units, configuring and managing the FortiGate VPN policies, monitoring the status of the managed devices, viewing and analyzing the FortiGate logs, updating the virus and attack signatures, providing web filtering and email filter service to the licensed FortiGate units as a local FDS, firmware revision control and updating the firmware images of the managed units.

- *FortiManager QuickStart Guides*

These documents are included with your FortiManager system package. Use these document to install and begin working with the FortiManager system and FortiManager GUI.

- *FortiManager Online Help*

You can get online help from the FortiManager GUI. FortiManager online help contains detailed procedures for using the FortiManager GUI to configure and manage FortiGate units.

- *FortiManager CLI Reference*

This document describes how to use the FortiManager Command Line Interface (CLI) and contains references for all FortiManager CLI commands.

- *FortiManager Release Notes*

This document describes new features and enhancements in the FortiManager system for the release, and lists resolved and known issues. This document also defines supported platforms and firmware versions.

- *FortiManager VM Install Guide*

This document describes installing FortiManager VM in your virtual environment.

What's New in FortiManager version 5.0

FortiManager version 5.0.12

No changes to the CLI have been made in FortiManager 5.0.12.

FortiManager version 5.0.11

The table below lists commands which have changed in FortiManager version 5.0.11.

Command	Change
<code>config system locallog ... filter</code>	Variable added: <code>devops</code>
<code>config system log settings</code>	Variable added: <code>sync-search-timeout</code>
<code>diagnose cdb check</code>	Variable added: <code>reference-integrity</code>

FortiManager version 5.0.10

The table below lists commands which have changed in FortiManager version 5.0.10.

Command	Change
<code>config system admin profile</code>	Variable added: <code>show-checkbox-in-table</code>
<code>config system log settings</code>	Variable added: <code>log-file-archive-name</code>
<code>config system report group</code>	Command added.
<code>config system report settings</code>	Variables added: <code>report-priority</code> <code>hcache-lossless</code>

Command	Change
<code>config system sql</code>	Variable removed: <code>auto-table-upgrade</code>
<code>config system sql</code>	Variables added: <code>device-count-high</code> <code>event-table-partition-time</code> <code>traffic-table-partition-time</code> <code>utm-table-partition-time</code>
<code>diagnose cdb check update-devinfo</code>	Command added.
<code>diagnose sql status rebuild-db</code> <code>diagnose sql status sql_hcache_chk</code>	Commands added.
<code>execute fmpolicy</code>	Commands added: <code>check-upgrade-object</code> <code>copy-adom-object</code> <code>install-config</code> <code>print-adom-database</code> <code>print-adom-object</code> <code>print-adom-package</code> <code>print-prov-templates</code> Commands removed: <code>print-global-database</code> <code>print-global object</code> <code>print global-package</code>
<code>execute sql-report</code>	Variables added: <code>list</code> <code>view</code> <code>hcache-check</code> <code>list-schedule</code>

FortiManager version 5.0.9

The table below lists commands which have changed in FortiManager version 5.0.9.

Command	Change
<code>config system global</code>	Variable added: <code>ssl-protocol</code>

FortiManager version 5.0.8

The table below lists commands which have changed in FortiManager version 5.0.8.

Command	Change
<code>config system admin profile</code>	Variable added: <code>change-password</code>
<code>config system admin setting</code>	Variable added: <code>admin-https-redirect</code>
<code>config system admin user</code>	Variable added: <code>change-password</code>
<code>config system ha</code>	Variable added: <code>file-quota</code>
<code>config system log settings</code>	Variable added: <code>FSA-custom-field1</code>
<code>config system report auto-cache</code>	Variables added: <code>aggressive-schedule</code> <code>drilldown-status, order</code>
<code>config system report settings</code>	Variable added: <code>max-table-rows</code>
<code>diagnose debug reset</code>	Command added.
<code>diagnose sql config top-dev set</code>	Command added.
<code>diagnose sql rebuild-report-hcache</code>	Command added.
<code>execute devicelog clear</code>	Command removed.

FortiManager version 5.0.7

The table below lists commands which have changed in FortiManager version 5.0.7.

Command	Change
<code>config system admin ldap</code>	Variable added: adom connect-timeout
<code>config system admin profile</code>	Variables added: type web-filter ips-filter app-filter workflow-approve
<code>config system admin user</code>	Variables added: web-filter ips-filter app-filter
<code>config system auto-delete</code>	Variable renamed: regular-auto-deletion to log-auto-deletion
<code>config system certificate</code>	Command added: oftp
<code>config system global</code>	Variable added: task-list-size Variable updated: workspace-mode Variable removed: swapmem
<code>config system locallog [syslogd syslogd2 syslogd3] setting</code>	Variables added: syslog-name Variables removed: server port
<code>config system locallog [memory disk fortianalyzer syslogd syslogd2 syslogd3] filter</code>	Variable added: faz

Command	Change
<code>config system log settings</code>	Variables removed: <ul style="list-style-type: none"> FGT-custom-field2 .. 5 FCT-custom-field2 .. 5 FML-custom-field2 .. 5 FWB-custom-field2 .. 5 FCH-custom-field2 .. 5 FAZ-custom-field2 .. 5
<code>config system sql</code>	Variables removed: <ul style="list-style-type: none"> event-table-partition-time event-table-partition-time-max event-table-partition-time-min table-partition-mode traffic-table-partition-time traffic-table-partition-time-max traffic-table-partition-time-min utm-table-partition-time utm-table-partition-time-max utm-table-partition-time-min
<code>diagnose debug application</code>	Variables added: <ul style="list-style-type: none"> dmworker curl
<code>diagnose dvm extender</code>	Command added: <ul style="list-style-type: none"> extender
<code>diagnose fortilogd</code>	Variable added: <ul style="list-style-type: none"> lograte
<code>diagnose report</code>	Variable removed: <ul style="list-style-type: none"> maintain
<code>execute remove <reports></code>	Variable added: <ul style="list-style-type: none"> device-id
<code>execute sql-report</code>	Variables added: <ul style="list-style-type: none"> list-lang import-lang

FortiManager version 5.0.6

The table below lists commands which have changed in FortiManager version 5.0.6.

Command	Change
<code>config fmupdate device-version</code>	Variable added: fsa
<code>config fmupdate web-spam fsa server-override</code>	Command added.
<code>config system admin ldap</code>	Variable added: attributes
<code>config system global</code>	Variable removed: webservice-support-ssl3
<code>config system global</code>	Variable added: webservice-proto
<code>config system report setting</code>	Command added.
<code>config system sql</code>	Variables added: rebuild-event rebuils-event-start-time
<code>diagnose debug application</code>	Variable added: ipsec Variable removed: ike
<code>diagnose dvm device</code>	Variable added: delete
<code>diagnose sql</code>	Variable added: remove query-cache
<code>diagnose test application fazautormd</code>	Command added.
<code>diagnose vpn tunnel</code>	Command added.
<code>execute auto-delete</code>	Command added.
<code>execute fmpolicy print-global-package</code>	Command added.

FortiManager version 5.0.5

The table below lists commands which have changed in FortiManager version 5.0.5.

Command	Change
<code>config fmupdate service</code>	Variable added: query-filequery
<code>config fmupdate web-spam fgd-setting</code>	Variables added: fq-cache fq-log fq-preload restrict-fq-dbver
<code>config system global</code>	Variables added: partial-install search-all-adoms faz-status unregister-pop-up
<code>config system log settings</code>	Variables added: FAZ-custom-field1 FAZ-custom-field2 FAZ-custom-field3 FAZ-custom-field4 FAZ-custom-field5
<code>diagnose fmupdate</code>	Variables removed: fgd-delwfdb fgd-delasdb fgd-delavquerydb
<code>execute backup</code>	Variable added: logs-rescue

FortiManager version 5.0.4

The table below lists commands which have changed in FortiManager version 5.0.4.

Command	Change
<code>config system auto-delete</code>	Command added.

Command	Change
<code>config system global</code>	Variable added: <code>log-checksum</code>
<code>config system log setting</code> <code>config rolling-regular</code>	Variable added: <code>upload-mode backup</code>
<code>config system report auto-cache</code>	Command added.
<code>config system report est-browse time</code>	Command added.
<code>config system sql</code>	Command added.
<code>diagnose report status</code> <code>diagnose report clean</code> <code>diagnose report maintain</code>	Commands added.
<code>diagnose sql auto-hcache</code>	Command removed.
<code>diagnose sql show log-filters</code>	Command added.
<code>execute log device permissions</code>	Command added.
<code>execute log import</code>	Command added.
<code>execute log-integrity</code>	Command added

FortiManager version 5.0.3

The table below lists commands which have changed in FortiManager version 5.0.3.

Command	Change
<code>config fmupdate service</code>	Variables added: <code>query-antispam</code> <code>query-antivirus</code> <code>query-webfilter</code>

Command	Change
<code>config fmupdate web-spam fgd-setting</code>	Variables added: <ul style="list-style-type: none"> linkd-log max-unrated-size restrict-as1-dbver restrict-as2-dbver restrict-as4-dbver restrict-av-dbver restrict-wf-dbver stat-sync-interval
<code>config system admin profile</code>	Variables added: <ul style="list-style-type: none"> fgd_center reports logs Variable removed: <ul style="list-style-type: none"> forticonsole
<code>config system admin setting</code>	Variables added: <ul style="list-style-type: none"> show_adom_forticonsole_button show_adom_implicit_id_based_policy show_schedule_script
<code>config system admin user</code>	Variables added: <ul style="list-style-type: none"> ip_trustedhost4 to ipvtrushost10 ipv6_trustedhost4 to ipv6_trusthost10 group password-expire force-password-change subject ca, two-factor-auth num-entries
<code>config system admin user dashboard</code>	Variables added: <ul style="list-style-type: none"> log-rate-type log-rate-topn log-rate-period res-view-type res-period res-cpu-display
<code>config system certificate crl</code>	Command added.

Command	Change
<code>config system dm</code>	Variable added: <code>fortiap-refresh-itvl</code>
<code>config system global</code>	Variables added: <code>adom-rev-max-days</code> <code>adom-rev-max-revisions</code> <code>dh-params</code> <code>lock-preempt</code> <code>pre-login-banner-message</code>
<code>config system locallog ... filter</code>	Variable added: <code>fmgws</code>
<code>config system log settings</code>	Variables added: <code>FCH-custom-field1 .. 5</code> <code>FCT-custom-field1 .. 5</code> <code>FGT-custom-field1 .. 5</code> <code>FML-custom-field1 .. 5</code> <code>FWB-custom-field1 .. 5</code>
<code>config system log settings rolling-regular</code>	Variables added: <code>days</code> <code>del-files</code> <code>directory</code> <code>file-size</code> <code>gzip-format</code> <code>hours</code> <code>ip</code> <code>log-format</code> <code>min</code> <code>password</code> <code>server-type</code> <code>upload</code> <code>upload-hour</code> <code>upload-trigger</code> <code>username</code> <code>when</code>
<code>config system report</code>	Command added.
<code>config system snmp sysinfo</code>	Variable added: <code>trap-cpu-high-exclude-nice-threshold</code>

Command	Change
<code>config system snmp user events</code>	Variable added: <ul style="list-style-type: none"> <code>cpu-high-exclude-nice</code> <code>lic-dev-quota</code> <code>lic-gbday</code> <code>log-alert</code> <code>log-data-rate</code> <code>log-rate</code>
<code>config system sql</code>	Variables added: <ul style="list-style-type: none"> <code>database-name</code> <code>event-table-partition-time</code> <code>event-table-partition-time-max</code> <code>event-table-partition-time-min</code> <code>reset</code> <code>resend-device</code> <code>server</code> <code>table-partition-mode</code> <code>traffic-table-partition-time</code> <code>traffic-table-partition-time-max</code> <code>traffic-table-partition-time-min</code> <code>username</code> <code>utm-table-partition-time</code> <code>utm-table-partition-time-max</code> <code>utm-table-partition-time-min</code>
<code>config system sql custom-index</code>	Variables added: <ul style="list-style-type: none"> <code>device-type</code> <code>log-type</code> <code>index-field</code>
<code>diagnose debug service</code>	Command added.
<code>diagnose dlp-archives</code>	Command added.
<code>diagnose dvm capability</code>	Command added.
<code>diagnose dvm device</code>	Variable removed: <ul style="list-style-type: none"> <code>deps</code>

Command	Change
<code>diagnose fmupdate</code>	Variables added: <code>dellog</code> <code>fgd-wfserver-stat</code> <code>show-dev-obj</code> Variable removed: <code>fml-bandwidth</code>
<code>diagnose pm2</code>	Command added.
<code>diagnose rtm</code>	Command removed.
<code>diagnose sql</code>	Variable added: <code>upload</code>
<code>diagnose system</code>	Variable added: <code>geoip</code> Variables removed: <code>disk</code> <code>logtoconsole</code> <code>raid</code>
<code>diagnose system admin-session</code>	Variable added: <code>kill</code>
<code>diagnose system export</code>	Variable added: <code>fmwslog</code>
<code>diagnose test application</code>	Variable added: <code>fazsvcd</code>
<code>diagnose test connection</code>	Command added.
<code>execute backup</code>	Variables added: <code>logs</code> <code>logs-only</code> <code>reports</code> <code>reports-config</code>
<code>get system report</code>	Command added.

Using the Command Line Interface

This chapter explains how to connect to the Command Line Interface (CLI) and describes the basics of using the CLI. You can use CLI commands to view all system information and to change all system configuration settings.

This chapter describes:

- CLI command syntax
- Connecting to the CLI
- CLI objects
- CLI command branches
- CLI basics

CLI command syntax

This guide uses the following conventions to describe command syntax.

- Angle brackets < > indicate variables.
- Vertical bar and curly brackets { | } separate alternative, mutually exclusive required variables.

For example:

```
set protocol {ftp | sftp}
```

You can enter `set protocol ftp` or `set protocol sftp`.

- Square brackets [] indicate that a variable is optional.

For example:

```
show system interface [<name_str>]
```

To show the settings for all interfaces, you can enter `show system interface`. To show the settings for the Port1 interface, you can enter `show system interface port1`.

- A space separates options that can be entered in any combination and must be separated by spaces.

For example:

```
set allowaccess {https ping ssh snmp telnet http webservice aggregator}
```

You can enter any of the following:

```
set allowaccess ping
set allowaccess https
set allowaccess ssh
set allowaccess https ssh
set allowaccess aggregator http https ping ssh telnet webservice
```

In most cases to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.

- Special characters:
 - The \ is supported to escape spaces or as a line continuation character.
 - The single quotation mark ' and the double quotation mark " are supported, but must be used in pairs.

- If there are spaces in a string, you must precede the spaces with the \ escape character or put the string in a pair of quotation marks.

Connecting to the CLI

You can use a directconsole connection orSSH to connect to the FortiManager CLI. You can also access through the CLI console widget on the GUI. For more information, see the FortiManager *Administration Guide*, and your device's QuickStart Guide.

You can use a direct console connection or SSH to connect to the FortiManager CLI.

Connecting to the FortiManager console

To connect to the FortiManager console, you need:

- a computer with an available communications port
- a console cable, provided with your FortiManager unit, to connect the FortiManager console port and a communications port on your computer
- terminal emulation software, such as HyperTerminal for Windows.



The following procedure describes how to connect to the FortiManager CLI using Windows HyperTerminal software. You can use any terminal emulation program.

To connect to the CLI:

1. Connect the FortiManager console port to the available communications port on your computer.
2. Make sure the FortiManager unit is powered on.
3. Start HyperTerminal, enter a name for the connection, and select OK.
4. Configure HyperTerminal to connect directly to the communications port on the computer to which you have connected the FortiManager console port.
5. Select *OK*.
6. Select the following port settings and select *OK*.

COM port	COM1
Bits per second	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

7. Press `Enter` to connect to the FortiManager CLI. A login prompt appears.
8. Type a valid administrator name and press `Enter`.
9. Type the password for this administrator and press `Enter`. A command prompt appears.

You have connected to the FortiManager CLI, and you can enter CLI commands.

Setting administrative access on an interface

To perform administrative functions through a FortiManager network interface, you must enable the required types of administrative access on the interface to which your management computer connects. Access to the CLI requires Secure Shell (SSH) access. If you want to use the GUI, you need HTTPS access.

To use the GUI to configure FortiManager interfaces for SSH access, see the [FortiManager Administration Guide](#).

To use the CLI to configure SSH access:

1. Connect and log into the CLI using the FortiManager console port and your terminal emulation software.
2. Use the following command to configure an interface to accept SSH connections:

```
config system interface
  edit <interface_name>
    set allowaccess <access_types>
  end
```

Where `<interface_name>` is the name of the FortiManager interface to be configured to allow administrative access, and `<access_types>` is a whitespace-separated list of access types to enable.

For example, to configure port1 to accept HTTPS and SSH connections, enter:

```
config system interface
  edit port1
    set allowaccess https ssh
  end
```



Remember to press `Enter` at the end of each line in the command example. Also, type `end` and press `Enter` to commit the changes to the FortiManager configuration.

3. To confirm that you have configured SSH access correctly, enter the following command to view the access settings for the interface:

```
get system interface <interface_name>
```

The CLI displays the settings, including the management access settings, for the named interface.

Connecting to the FortiManager CLI using SSH

SSH provides strong secure authentication and secure communications to the FortiManager CLI from your internal network or the internet. Once the FortiManager unit is configured to accept SSH connections, you can run an SSH client on your management computer and use this client to connect to the FortiManager CLI.

To connect to the CLI using SSH:

1. Install and start an SSH client.
2. Connect to a FortiManager interface that is configured for SSH connections.
3. Type a valid administrator name and press `Enter`.
4. Type the password for this administrator and press `Enter`.

The FortiManager model name followed by a # is displayed.

You have connected to the FortiManager CLI, and you can enter CLI commands.

Connecting to the FortiManager CLI using the GUI

The GUI also provides a CLI console window.

To connect to the CLI using the GUI:

1. Connect to the GUI and log in.
2. Go to *System Settings > Dashboard*
3. Click inside the CLI Console widget. If the widget is not available, select *Add Widget* to add the widget to the dashboard.

CLI objects

The FortiManager CLI is based on configurable objects. The top-level objects are the basic components of FortiManager functionality.

system	Configuration options related to the overall operation of the FortiManager unit, such as interfaces, virtual domains, and administrators.
fmupdate	Configures settings related to FortiGuard service updates and the unit's built-in FDS.

This object contains more specific lower level objects. For example, the system object contains objects for administrators, DNS, interfaces and so on.

CLI command branches

The FortiManager CLI consists of the following command branches:

config branch	execute branch
get branch	diagnose branch
show branch	

Examples showing how to enter command sequences within each branch are provided in the following sections.

config branch

The `config` commands configure objects of FortiManager functionality. Top-level objects are not configurable, they are containers for more specific lower level objects. For example, the system object contains administrators, DNS addresses, interfaces, routes, and so on. When these objects have multiple sub-objects, such as administrators or routes, they are organized in the form of a table. You can add, delete, or edit the entries in the table. Table entries each consist of variables that you can set to particular values. Simpler objects, such as system DNS, are a single set of variables.

To configure an object, you use the `config` command to navigate to the object's command "shell". For example, to configure administrators, you enter the command

```
config system admin user
```

The command prompt changes to show that you are in the admin shell.

```
(user) #
```

This is a table shell. You can use any of the following commands:

edit	Add an entry to the FortiManager configuration or edit an existing entry. For example in the <code>config system admin shell</code> : <ul style="list-style-type: none"> Type <code>edit admin</code> and press <code>Enter</code> to edit the settings for the default admin administrator account. Type <code>edit newadmin</code> and press <code>Enter</code> to create a new administrator account with the name <code>newadmin</code> and to edit the default settings for the new administrator account.
delete	Remove an entry from the FortiManager configuration. For example in the <code>config system admin shell</code> , type <code>delete newadmin</code> and press <code>Enter</code> to delete the administrator account named <code>newadmin</code> .
purge	Remove all entries configured in the current shell. For example in the <code>config user local shell</code> : <ul style="list-style-type: none"> Type <code>get</code> to see the list of user names added to the FortiManager configuration, Type <code>purge</code> and then <code>y</code> to confirm that you want to purge all the user names, Type <code>get</code> again to confirm that no user names are displayed.
get	List the configuration. In a table shell, <code>get</code> lists the table members. In an edit shell, <code>get</code> lists the variables and their values.
show	Show changes to the default configuration as configuration commands.
end	Save the changes you have made in the current shell and leave the shell. Every <code>config</code> command must be paired with an <code>end</code> command. You will return to the root FortiManager CLI prompt. The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell.

If you enter the `get` command, you see a list of the entries in the table of administrators. To add a new administrator, you enter the `edit` command with a new administrator name:

```
edit admin_1
```

The FortiManager unit acknowledges the new table entry and changes the command prompt to show that you are now editing the new entry:

```
new entry 'admin_1' added
(admin_1) #
```

From this prompt, you can use any of the following commands:

config	In a few cases, there are subcommands that you access using a second <code>config</code> command while editing a table entry. An example of this is the command to add restrict the user to specific devices or VDOMs.
---------------	--

set	Assign values. For example from the <code>edit admin</code> command shell, typing <code>set password newpass</code> changes the password of the admin administrator account to <code>newpass</code> . When using a <code>set</code> command to make changes to lists that contain options separated by spaces, you need to retype the whole list including all the options you want to apply and excluding all the options you want to remove.
unset	Reset values to defaults. For example from the <code>edit admin</code> command shell, typing <code>unset password</code> resets the password of the admin administrator account to the default of no password.
get	List the configuration. In a table shell, <code>get</code> lists the table members. In an edit shell, <code>get</code> lists the variables and their values.
show	Show changes to the default configuration in the form of configuration commands.
next	Save the changes you have made in the current shell and continue working in the shell. For example if you want to add several new admin user accounts enter the <code>config system admin user</code> shell. <ul style="list-style-type: none"> • Type <code>edit User1</code> and press <code>Enter</code>. • Use the <code>set</code> commands to configure the values for the new admin account. • Type <code>next</code> to save the configuration for User1 without leaving the <code>config system admin user</code> shell. • Continue using the <code>edit</code>, <code>set</code>, and <code>next</code> commands to continue adding admin user accounts. • Type <code>end</code> and press <code>Enter</code> to save the last configuration and leave the shell.
abort	Exit an edit shell without saving the configuration.
end	Save the changes you have made in the current shell and leave the shell. Every <code>config</code> command must be paired with an <code>end</code> command. The <code>end</code> command is also used to save <code>set</code> command changes and leave the shell.

The `config` branch is organized into configuration shells. You can complete and save the configuration within each shell for that shell, or you can leave the shell without saving the configuration. You can only use the configuration commands for the shell that you are working in. To use the configuration commands for another shell you must leave the shell you are working in and enter the other shell.

get branch

Use `get` to display settings. You can use `get` within a `config` shell to display the settings for that shell, or you can use `get` with a full path to display the settings for the specified shell.

To use `get` from the root prompt, you must include a path to a shell.

The root prompt is the FortiManager host or model name followed by a number sign (#).

Example 1

When you type `get` in the `config system admin user` shell, the list of administrators is displayed.

At the `(user) #` prompt, type:


```
get
```

The screen displays:

```
== [ admin ]
userid: admin
== [ admin2 ]
userid: admin2
== [ admin3 ]
userid: admin3
```

Example 2

When you type `get` in the `admin` user shell, the configuration values for the `admin` administrator account are displayed.

```
edit admin
```

At the `(admin) #` prompt, type:

```
get
```

The screen displays:

```
userid : admin
password : *
trusthost1 : 0.0.0.0 0.0.0.0
trusthost2 : 0.0.0.0 0.0.0.0
trusthost3 : 0.0.0.0 0.0.0.0
trusthost4 : 0.0.0.0 0.0.0.0
trusthost5 : 0.0.0.0 0.0.0.0
trusthost6 : 0.0.0.0 0.0.0.0
trusthost7 : 0.0.0.0 0.0.0.0
trusthost8 : 0.0.0.0 0.0.0.0
trusthost9 : 0.0.0.0 0.0.0.0
trusthost10 : 127.0.0.1 255.255.255.255
ipv6_trusthost1 : ::/0
ipv6_trusthost2 : ::/0
ipv6_trusthost3 : ::/0
ipv6_trusthost4 : ::/0
ipv6_trusthost5 : ::/0
ipv6_trusthost6 : ::/0
ipv6_trusthost7 : ::/0
ipv6_trusthost8 : ::/0
ipv6_trusthost9 : ::/0
ipv6_trusthost10 : ::1/128
profileid : Super_User
adom:
  == [ all_adoms ]
  adom-name: all_adoms
policy-package:
  == [ all_policy_packages ]
  policy-package-name: all_policy_packages
restrict-access : disable
restrict-dev-vdom:
description : (null)
user_type : local
ssh-public-key1 :
ssh-public-key2 :
ssh-public-key3 :
meta-data:
```

```
last-name : (null)
first-name : (null)
email-address : (null)
phone-number : (null)
mobile-number : (null)
pager-number : (null)
hidden : 0
dashboard-tabs:
dashboard:
  == [ 6 ]
  moduleid: 6
  == [ 1 ]
  moduleid: 1
  == [ 2 ]
  moduleid: 2
  == [ 3 ]
  moduleid: 3
  == [ 4 ]
  moduleid: 4
  == [ 5 ]
  moduleid: 5
```

Example 3

You want to confirm the IP address and netmask of the port1 interface from the root prompt.

At the (command) # prompt, type:

```
get system interface port1
```

The screen displays:

```
name : port1
status : up
ip : 172.16.81.30 255.255.255.0
allowaccess : ping https ssh snmp telnet http webservice aggregator
serviceaccess :
speed : auto
description : (null)
alias : (null)
ipv6:
  ip6-address: ::/0 ip6-allowaccess:
```

show branch

Use `show` to display the FortiManager unit configuration. Only changes to the default configuration are displayed. You can use `show` within a `config` shell to display the configuration of that shell, or you can use `show` with a full path to display the configuration of the specified shell.

To display the configuration of all `config` shells, you can use `show` from the root prompt. The root prompt is the FortiManager host or model name followed by a number sign (#).

Example 1

When you type `show` and press `Enter` within the `port1` interface shell, the changes to the default interface configuration are displayed.

At the `(port1) #` prompt, type:

```
show
```

The screen displays:

```
config system interface
  edit "port1"
    set ip 172.16.81.30 255.255.255.0
    set allowaccess ping https ssh snmp telnet http webservice aggregator
  next
  edit "port2"
    set ip 1.1.1.1 255.255.255.0
    set allowaccess ping https ssh snmp telnet http webservice aggregator
  next
  edit "port3"
  next
  edit "port4"
  next
end
```

Example 2

You are working in the `port1` interface shell and want to see the `system dns` configuration. At the `(port1) #` prompt, type:

```
show system dns
```

The screen displays:

```
config system dns
  set primary 65.39.139.53
  set secondary 65.39.139.63
end
```

execute branch

Use `execute` to run static commands, to reset the FortiManager unit to factory defaults, or to back up or restore the FortiManager configuration. The execute commands are available only from the root prompt.

The root prompt is the FortiManager host or model name followed by a number sign (#).

Example

At the root prompt, type:

```
execute reboot
The system will be rebooted.
Do you want to continue? (y/n)
```

and press `Enter` to restart the FortiManager unit.

diagnose branch

Commands in the `diagnose` branch are used for debugging the operation of the FortiManager unit and to set parameters for displaying different levels of diagnostic information.



Diagnose commands are intended for advanced users only. Contact Fortinet Technical Support before using these commands.

Example command sequences



The command prompt changes for each shell.

To configure the primary and secondary DNS server addresses:

1. Starting at the root prompt, type:

```
config system dns
```

and press Enter. The prompt changes to (dns) #.

2. At the (dns) # prompt, type (question mark) ?

The following options are displayed.

```
set
unset
get
show
abort
end
```

3. Type set ?

The following options are displayed:

```
primary
secondary
```

4. To set the primary DNS server address to 172.16.100.100, type:

```
set primary 172.16.100.100
```

and press Enter.

5. To set the secondary DNS server address to 207.104.200.1, type:

```
set secondary 207.104.200.1
```

and press Enter.

6. To restore the primary DNS server address to the default address, type unset primary and press Enter.

7. If you want to leave the config system dns shell without saving your changes, type abort and press Enter.

8. To save your changes and exit the dns sub-shell, type end and press Enter.

9. To confirm your changes have taken effect after leaving the dns sub-shell, type get system dns and press Enter.

CLI basics

Command help

You can press the question mark (?) key to display command help.

- Press the question mark (?) key at the command prompt to display a list of the commands available and a description of each command.

- Type a command followed by a space and press the question mark (?) key to display a list of the options available for that command and a description of each option.
- Type a command followed by an option and press the question mark (?) key to display a list of additional options available for that command option combination and a description of each option.

Command tree

Type `tree` to display the FortiManager CLI command tree. To capture the full output, connect to your device using a terminal emulation program, such as PuTTY, and capture the output to a log file. For `config` commands, use the `tree` command to view all available variables and sub-commands.

Example

```
#config system interface
(interface)# tree
-- [interface] --*name
    |- status
    |- ip
    |- allowaccess
    |- serviceaccess
    |- speed
    |- description
    |- alias
    +- <ipv6> -- ip6-address
        +- ip6-allowaccess
```

Command completion

You can use the tab key or the question mark (?) key to complete commands:

- You can press the tab key at any prompt to scroll through the options available for that prompt.
- You can type the first characters of any command and press the tab key or the question mark (?) key to complete the command or to scroll through the options that are available at the current cursor position.
- After completing the first word of a command, you can press the space bar and then the tab key to scroll through the options available at the current cursor position.

Recalling commands

You can recall previously entered commands by using the Up and Down arrow keys to scroll through commands you have entered.

Editing commands

Use the left and right arrow keys to move the cursor back and forth in a recalled command. You can also use the backspace and delete keys and the control keys listed in the following table to edit the command.

Function	Key combination
Beginning of line	Control key + A

Function	Key combination
End of line	Control key + E
Back one character	Control key + B
Forward one character	Control key + F
Delete current character	Control key + D
Previous command	Control key + P
Next command	Control key + N
Abort the command	Control key + C
If used at the root prompt, exit the CLI	Control key + C

Line continuation

To break a long command over multiple lines, use a \ at the end of each line.

Command abbreviation

You can abbreviate commands and command options to the smallest number of unambiguous characters. For example, the command `get system status` can be abbreviated to `g sy st.`

Environment variables

The FortiManager CLI supports several environment variables.

\$USERFROM	The management access type (SSH, Telnet and so on) and the IP address of the logged in administrator.
\$USERNAME	The user account name of the logged in administrator.
\$SerialNum	The serial number of the FortiManager unit.

Variable names are case sensitive. In the following example, when entering the variable, you can type (dollar sign) `$` followed by a tab to auto-complete the variable to ensure that you have the exact spelling and case. Continue pressing tab until the variable you want to use is displayed.

```
config system global
    set hostname $SerialNum
end
```

Encrypted password support

After you enter a clear text password using the CLI, the FortiManager unit encrypts the password and stores it in the configuration file with the prefix ENC. For example:

```
show system admin user user1
config system admin user
    edit "user1"
        set password ENC UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1
        rVJmMFc9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQxskRcU3E9XqOit82PgScwzGzGuJ5a9
        f
        set profileid "Standard_User"
    next
end
```

It is also possible to enter an already encrypted password. For example, type:

```
config system admin
then press Enter.
```

Type:

```
edit user1
then press Enter.
```

Type:

```
set password ENC UAGUDZ1yEaG30620s6afD3Gac1FnOT0BC1rVJmMF
c9ubLlW4wEvHcqGVq+ZnrgbudK7aryyf1scXcXdnQxskRcU3E9XqOit82PgScwzGzGuJ5a9f
then press Enter.
```

Type:

```
end
then press Enter.
```

Entering spaces in strings

When a string value contains a space, do one of the following:

- Enclose the string in quotation marks, for example "Security Administrator".
- Enclose the string in single quotes, for example 'Security Administrator'.
- Use a backslash ("\") preceding the space, for example Security\ Administrator.

Entering quotation marks in strings

If you want to include a quotation mark, single quote or apostrophe in a string, you must precede the character with a backslash character. To include a backslash, enter two backslashes.

Entering a question mark (?) in a string

If you want to include a question mark (?) in a string, you must precede the question mark with CTRL-V. Entering a question mark without first entering CTRL-V causes the CLI to display possible command completions, terminating the string.

International characters

The CLI supports international characters in strings.

Special characters

The characters <, >, (,), #, ', and " are not permitted in most CLI fields, but you can use them in passwords. If you use the apostrophe (') or quote (") character, you must precede it with a backslash (\) character when entering it in the CLI `set` command.

IP address formats

You can enter an IP address and subnet using either dotted decimal or slash-bit format. For example you can type one of:

```
set ip 192.168.1.1 255.255.255.0
set ip 192.168.1.1/24
```

The IP address is displayed in the configuration file in dotted decimal format.

Editing the configuration file

You can change the FortiManager configuration by backing up the configuration file to a FTP, SCP, or SFTP server. Then you can make changes to the file and restore it to the FortiManager unit.

1. Use the `execute backup all-settings` command to back up the configuration file to a FTP server. For example,

```
execute backup all-settings ftp 10.10.0.1 mybackup.cfg myid mypass
```

2. Edit the configuration file using a text editor.

Related commands are listed together in the configuration file. For instance, all the system commands are grouped together. You can edit the configuration by adding, changing or deleting the CLI commands in the configuration file.

The first line of the configuration file contains information about the firmware version and FortiManager model. Do not edit this line. If you change this information the FortiManager unit will reject the configuration file when you attempt to restore it.

3. Use the `execute restore all-settings` command to copy the edited configuration file back to the FortiManager unit. For example,

```
execute restore all-settings 10.10.0.1 mybackup.cfg myid mypass
```

The FortiManager unit receives the configuration file and checks to make sure the firmware version and model information is correct. If it is, the FortiManager unit loads the configuration file and checks each command for errors. If the FortiManager unit finds an error, an error message is displayed after the command and the command is rejected. Then the FortiManager unit restarts and loads the new configuration.

Changing the baud rate

Using `execute console baudrate`, you can change the default console connection baud rate.

To check the current baud rate enter the following CLI command:

```
# execute console baudrate [enter]
```



```
current baud rate is: 9600
```

To view baudrate options, enter the CLI command with the question mark (?).

```
# execute console baudrate ?  
baudrate 9600 | 19200 | 38400 | 57600 | 115200
```

To change the baudrate, enter the CLI command as listed below.

```
# execute console baudrate 19200  
Your console connection will get lost after changing baud rate.  
Change your console setting!  
Do you want to continue? (y/n)
```



Changing the default baud rate is not available on all models.

Debug log levels

The following table lists available debug log levels on your FortiManager .

Level	Type	Description
0	Emergency	The system has become unusable.
1	Alert	Immediate action is required.
2	Critical	Functionality is affected.
3	Error	An erroneous condition exists and functionality is probably affected.
4	Warning	Function might be affected.
5	Notice	Notification of normal events.
6	Information	General information about system operations.
7	Debug	Detailed information useful for debugging purposes.
8	Maximum	Maximum log level.

Administrative Domains

This chapter provides information about the ADOM functionality in FortiManager.

ADOMs overview

FortiManager can manage a large number of Fortinet devices. ADOMs enable administrators to manage only those devices that are specific to their geographic location or business division. This also includes FortiGate units with multiple configured VDOMs.

If ADOMs are enabled, each administrator account is tied to an administrative domain. When a particular administrator logs in, they see only those devices or VDOMs that have been enabled for their account. The one exception is the `admin` administrator account which can see and maintain all administrative domains and the devices within those domains.

Administrative domains are not enabled by default, and enabling and configuring the domains can only be performed by the `admin` administrator.

The default and maximum number of administrative domains you can add depends on the FortiManager system model. The table below outlines these limits.

FortiManager Model	Administrative Domain / Network Devices
FMG-100C	30 / 30
FMG-200D	30 / 30
FMG-300D	300 / 300
FMG-400B	300 / 300
FMG-400C	300 / 300
FMG-1000C	800 / 800
FMG-1000D	1000 / 1000
FMG-3000B	5000 / 5000
FMG-3000C	5000 / 5000
FMG-4000D	4000 / 4000
FMG-4000E	4000 / 4000
FMG-5001A	4000 / 4000

FortiManager Model	Administrative Domain / Network Devices
FMG-VM-Base	10/10
FMG-VM-10-UG	+10/+10
FMG-VM-100-UG	+100/+100
FMG-VM-1000-UG	+1000/+1000
FMG-VM-5000-UG	+5000/+5000
FMG-VM-U-UG	+10000/+10000

Configuring ADOMs

To use administrative domains, the `admin` administrator must first enable the feature, create ADOMs, and assign existing FortiManager administrators to ADOMs.



Enabling ADOMs moves non-global configuration items to the `root` ADOM. Back up the FortiManager unit configuration before enabling ADOMs.



ADOMs must be enabled before adding FortiMail, FortiWeb, and FortiCarrier devices to the FortiManager system. FortiMail and FortiWeb devices are added to their respective pre-configured ADOMs.



In FortiManager version 5.0.3 or later, FortiGate and FortiCarrier devices can no longer be grouped into the same ADOM. FortiCarrier devices should be grouped into a dedicated FortiCarrier ADOM.

Within the CLI, you can enable ADOMs and set the administrator ADOM. To configure the ADOMs, you must use the GUI.

To enable or disable ADOMs:

Enter the following CLI command:

```
config system global
    set adom-status {enable | disable}
end
```

An administrative domain has two modes: normal and advanced. Normal mode is the default device mode. In normal mode, a FortiGate unit can only be added to a single administrative domain. In advanced mode, you can assign different VDOMs from the same FortiGate to multiple administrative domains.



Enabling the advanced mode option will result in a reduced operation mode and more complicated management scenarios. It is recommended only for advanced users.

To change ADOM device modes:

Enter the following CLI command:

```
config system global
    set adom-mode {advanced | normal}
end
```

To assign an administrator to an ADOM:

Enter the following CLI command:

```
config system admin user
    edit <name>
        set adom <adom_name>
    next
end
```

where <name> is the administrator user name and <adom_name> is the ADOM name.

Concurrent ADOM Access

System administrators can enable or disable concurrent access to the same ADOM if multiple administrators are responsible for managing a single ADOM. When enabled, multiple administrators can log in to the same ADOM concurrently. When disabled, only a single administrator has read/write access to the ADOM, while all other administrators have read-only access.

Concurrent ADOM access can be enabled or disabled using the CLI.



Concurrent ADOM access is enabled by default. This can cause conflicts if two administrators attempt to make configuration changes to the same ADOM concurrently.

To enable ADOM locking and disable concurrent ADOM access:

```
config system global
    set workspace-mode normal
end
```

To disable ADOM locking and enable concurrent ADOM access:

```
config system global
    set workspace-mode disable
    Warning: disabling workspaces may cause some logged in users to lose their
    unsaved data. Do you want to continue? (y/n) y
end
```

To enable workspace workflow mode:

```
config system global
    set workspace-mode workflow
end
```



When workflow mode is enabled then the admin will have an extra option in the admin page under profile to allow the admin to approve or reject workflow requests.

system

Use system commands to configure options related to the overall operation of the FortiManager unit.



FortiManager CLI commands and variables are case sensitive.

admin

Use the following commands to configure administration related settings.

admin group

Use this command to add, edit, and delete administrative user groups.

Syntax

```
config system admin group
  edit <name>
    set <member>
  end
```

where `name` is the name of the group you are editing, and `member` are the group members.

admin ldap

Use this command to add, edit, and delete Lightweight Directory Access Protocol (LDAP) administrative users.

Syntax

```
config system admin ldap
  edit <name>
    set server {name_str | ip_str}
    set cnid <string>
    set dn <string>
    set port <integer>
    set type {anonymous | regular | simple}
    set username <string>
    set password <string>
    set group <string>
    set filter <query_string>
    set attributes <filter>
    set secure {disable | ldaps | starttls}
    set ca-cert <string>
    set connect-timeout <integer>
    set adom <adom-name>
  end
```

Variable	Description
<name>	Enter the name of the LDAP server or enter a new name to create an entry.
server {name_ str ip_ str}	Enter the LDAP server domain name or IP address. Enter a new name to create a new entry.
cnid <string>	Enter the common name identifier. Default: cn
dn <string>	Enter the distinguished name.
port <integer>	Enter the port number for LDAP server communication. Default: 389
type {anonymous regular simple}	Set a binding type: <ul style="list-style-type: none"> anonymous: Bind using anonymous user search regular: Bind using username/password and then search simple: Simple password authentication without search Default: simple
username <string>	Enter a username. This variable appears only when type is set to regular.
password <string>	Enter a password for the username above. This variable appears only when type is set to regular.
group <string>	Enter an authorization group. The authentication user must be a member of this group (full DN) on the server.
filter <query_ string>	Enter content for group searching. For example: <ul style="list-style-type: none"> (&(objectcategory=group) (member=*)) (&(objectclass=groupofnames) (member=*)) (&(objectclass=groupofuniquenames) (uniquemember=*)) (&(objectclass=posixgroup) (memberuid=*))
attributes <filter>	Attributes used for group searching (for multi-attributes, a use comma as a separator). For example: <ul style="list-style-type: none"> member uniquemember member,uniquemember
secure {disable ldaps starttls}	Set the SSL connection type: <ul style="list-style-type: none"> disable: No SSL ldaps: Use LDAPS starttls: Use STARTTLS

Variable	Description
ca-cert <string>	CA certificate name. This variable appears only when <code>secure</code> is set to <code>ldaps</code> or <code>starttls</code> .
connect-timeout <integer>	Set the LDAP connection timeout (msec).
adom <adom-name>	Set the ADOM name to link to the LDAP configuration.

Example

This example shows how to add the LDAP administrative user `user1` at the IP address `206.205.204.203`.

```
config system admin ldap
edit user1
set server 206.205.204.203
set dn techdoc
set type regular
set username auth1
set password auth1_pwd
set group techdoc
end
```

admin profile

Use this command to configure access profiles. In a newly-created administrative profile, no access is enabled.

Syntax

```
config system admin profile
edit <profile>
set description <text>
set type {restricted | system}
set web-filter {enable | disable}
set ips-filter {enable | disable}
set app-filter {enable | disable}
set scope
set system-setting {none | read | read-write}
set adom-switch {none | read | read-write}
set global-policy-packages {none | read | read-write}
set global-objects
set assignment {none | read | read-write}
set read-passwd {none | read | read-write}
set device-manager {none | read | read-write}
set device-config {none | read | read-write}
set device-op {none | read | read-write}
set device-profile {none | read | read-write}
set policy-objects {none | read | read-write}
set deploy-management {none | read | read-write}
set config-retrieve {none | read | read-write}
set term-access {none | read | read-write}
set adom-policy-packages {none | read | read-write}
set adom-policy-objects
set vpn-manager {none | read | read-write}
set realtime-monitor {none | read | read-write}
```

```

set consistency-check {none | read | read-write}
set faz-management
set log-viewer {none | read | read-write}
set report-viewer {none | read | read-write}
set event-management {none | read | read-write}
set change-password {enable | disable}
set fgd_center {none | read | read-write}
set workflow-approve {none | read | read-write}
set network
set admin
set system
set devices
set alerts
set dlp
set quar
set net-monitor
set vuln-mgmt
set reports
set logs
end

```

Variable	Description
<profile>	Edit the access profile. Enter a new name to create a new profile. The predefined access profiles are <i>Super_User</i> , <i>Standard_User</i> , <i>Restricted_User</i> , and <i>Package_User</i> .
description <text>	Enter a description for this access profile. Enclose the description in quotes if it contains spaces. The description can be up to 1023 characters.
type {restricted system}	Enter the admin profile type. One of: <ul style="list-style-type: none"> restricted: Restricted admin profile system: System admin profile
web-filter {enable disable}	Enable/disable Web Filter Profile permission for the restricted admin profile. Dependencies: type must be set to restricted
ips-filter {enable disable}	Enable/disable Application Sensor permission for the restricted admin profile. Dependencies: type must be set to restricted
app-filter {enable disable}	Enable/disable IPS Sensor permission for the restricted admin profile. Dependencies: type must be set to restricted
scope (Not Applicable)	CLI command is not in use.

Variable	Description
<pre>system-setting {none read read- write}</pre>	<p>Configure System Settings permissions for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the System Settings option in the GUI administrator profile.</p> <p>Controlled functions: System Settings tab, All the settings under System setting</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>
<pre>adom-switch {none read read- write}</pre>	<p>Configure administrative domain (ADOM) permissions for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>Controlled functions: ADOM settings in DVM, ADOM settings in All ADOMs page (under System Settings tab)</p> <p>Dependencies: If <code>system-setting</code> is <code>none</code>, the All ADOMs page is not accessible, <code>type</code> must be set to <code>system</code></p>
<pre>global-policy- packages {none read read- write}</pre>	<p>Configure global policy package permissions for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Global Policy Packages & Objects option in the GUI administrator profile. This is a sub-setting of <code>policy-objects</code>.</p> <p>Controlled functions: All operations in Global ADOM</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>
<pre>assignment {none read read- write}</pre>	<p>Configure assignment permissions for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Assignment option in the GUI administrator profile. This is a sub-setting of <code>policy-objects</code>.</p> <p>Controlled functions: Global assignment in Global ADOM</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>
<pre>read-passwd {none read read- write}</pre>	<p>Add the capability to view the authentication password in clear text to this profile.</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>
<pre>device-manager {none read read- write}</pre>	<p>Enter the level of access to Device Manager settings for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Device Manager option in the GUI administrator profile.</p> <p>Controlled functions: Device Manager tab</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>
<pre>device-config {none read read- write}</pre>	<p>Enter the level of access to device configuration settings for this profile.</p> <p>Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Manage Device Configuration option in the GUI administrator profile. This is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Edit devices, All settings under Menu in Dashboard</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>

Variable	Description
<pre>device-op {none read read- write}</pre>	<p>Add the capability to add, delete, and edit devices to this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Add/Delete Devices/Groups option in the GUI administrator profile. This is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Add or delete devices or groups</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>
<pre>device-profile {none read read- write}</pre>	<p>Configure device profile permissions for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the System Templates option in the GUI administrator profile. This is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Provisioning Templates</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>
<pre>policy-objects {none read read- write}</pre>	<p>This command corresponds to the Policy & Objects option in the GUI administrator profile.</p> <p>Controlled functions: Policy & Objects tab</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>
<pre>deploy-management {none read read- write}</pre>	<p>Enter the level of access to the deployment management configuration settings for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Install to Devices option in the GUI administrator profile. This is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Install to devices</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>
<pre>config-retrieve {none read read- write}</pre>	<p>Set the configuration retrieve settings for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Retrieve Configuration from Devices option in the GUI administrator profile. This is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Retrieve configuration from devices</p> <p>Dependencies: <code>deploy-management</code> must be set to <code>read-write</code> for <code>config-retrieve</code> to be set to <code>read-write</code>, <code>type</code> must be set to <code>system</code></p>
<pre>term-access {none read read- write}</pre>	<p>Set the terminal access permissions for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Terminal Access option in the GUI administrator profile. This is a sub-setting of <code>device-manager</code>.</p> <p>Controlled functions: Connect to the CLI via Telnet or SSH</p> <p>Dependencies: Depends on <code>device-config</code> option, <code>type</code> must be set to <code>system</code></p>

Variable	Description
<pre> adom-policy- packages {none read read- write} </pre>	<p>Enter the level of access to ADOM policy packages for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Policy Packages & Objects option in the GUI administrator profile. This is a sub-setting of <code>policy-objects</code>.</p> <p>Controlled functions: All the operations in ADOMs</p> <p>Dependencies: Install and re-install depends on Install to Devices in DVM settings, <code>type</code> must be set to <code>system</code></p>
<pre> vpn-manager {none read read- write} </pre>	<p>Enter the level of access to VPN console configuration settings for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the VPN Manager option in the GUI administrator profile. This is a sub-setting of <code>policy-objects</code>.</p> <p>Controlled functions: VPN Console</p> <p>Dependencies: VPN Management must be configured as Central VPN Console at ADOM level, Must be enabled in <i>System Settings > Admin settings</i>, <code>type</code> must be set to <code>system</code></p>
<pre> realtime-monitor {none read read- write} </pre>	<p>Enter the level of access to the Drill Down configuration settings for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Drill Down option in the GUI administrator profile.</p> <p>Controlled functions: Drill Down tab and all its operations</p> <p>Dependencies: <code>faz-status</code> must be set to <code>enable</code> in system global, <code>type</code> must be set to <code>system</code></p>
<pre> consistency-check {none read read- write} </pre>	<p>Configure Policy Check permissions for this profile. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Policy Check option in the GUI administrator profile.</p> <p>This is a sub-setting of <code>policy-objects</code>.</p> <p>Controlled functions: Policy check</p> <p>Dependencies: <code>type</code> must be set to <code>system</code></p>
<pre> log-viewer {none read read- write} </pre>	<p>Set the Log View permission. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Log View option in the GUI administrator profile.</p> <p>Controlled functions: Log View tab and all its operations</p> <p>Dependencies: <code>faz-status</code> must be set to <code>enable</code> in system global, <code>type</code> must be set to <code>system</code></p>
<pre> report-viewer {none read read- write} </pre>	<p>Set the Reports permission. Type <code>none</code> to hide this option from the administrator in the GUI.</p> <p>This command corresponds to the Reports option in the GUI administrator profile.</p> <p>Controlled functions: Reports tab and all its operations</p> <p>Dependencies: <code>faz-status</code> must be set to <code>enable</code> in system global, <code>type</code> must be set to <code>system</code></p>

Variable	Description
event-management {none read read- write}	Set the Event Management permission. Type <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the Event Management option in the GUI administrator profile. Controlled functions: Event Management tab and all its operations Dependencies: <code>faz-status</code> must be set to <code>enable</code> in system global, <code>type</code> must be set to <code>system</code>
change-password {enable disable}	Enable/disable allowing admin users to change their password.
fgd_center {none read read- write}	Set the FortiGuard Center permission. Type <code>none</code> to hide this option from the administrator in the GUI. This command corresponds to the FortiGuard Center option in the GUI administrator profile. Controlled functions: FortiGuard tab, All the settings under FortiGuard Dependencies: <code>type</code> must be set to <code>system</code>
workflow-approve {none read read- write}	Set the workspace workflow permission to approve workflow session requests. Type one of the following settings: <ul style="list-style-type: none"> • <code>none</code>: No permission. • <code>read</code>: Read permission. • <code>read-write</code>: Read-write permission. Dependencies: <code>type</code> must be set to <code>system</code>
adom-policy-objects	CLI command is not in use.
global-objects	CLI command is not in use.
faz-management	CLI command is not in use.
network	CLI command is not in use.
admin	CLI command is not in use.
system	CLI command is not in use.
devices	CLI command is not in use.
alerts	CLI command is not in use.
dlp	CLI command is not in use.
quar	CLI command is not in use.
net-monitor	CLI command is not in use.

Variable	Description
vuln-mgmt	CLI command is not in use.
reports	CLI command is not in use.
logs	CLI command is not in use.

admin radius

Use this command to add, edit, and delete administration RADIUS servers.

Syntax

```

config system admin radius
  edit <server>
    set auth-type <auth_prot_type>
    set nas-ip <ip>
    set port <integer>
    set secondary-secret <password_string>
    set secondary-server <string>
    set secret <password_string>
    set server <string>
  end

```

Variable	Description
<server>	Enter the name of the RADIUS server or enter a new name to create an entry.
auth-type <auth_prot_type>	Enter the authentication protocol the RADIUS server will use. <ul style="list-style-type: none"> any: use any supported authentication protocol mschap2 chap pap
nas-ip <ip>	Enter the NAS IP address.
port <integer>	Enter the RADIUS server port number. Default: 1812
secondary-secret <password_string>	Enter the password to access the RADIUS secondary-server.
secondary-server <string>	Enter the RADIUS secondary-server DNS resolvable domain name or IP address.
secret <password_string>	Enter the password to access the RADIUS server.
server <string>	Enter the RADIUS server DNS resolvable domain name or IP address.

Example

This example shows how to add the RADIUS server RAID1 at the IP address 206.205.204.203 and set the shared secret as R1a2D3i4U5s.

```
config system admin radius
  edit RAID1
    set server 206.205.204.203
    set secret R1a2D3i4U5s
  end
```

admin setting

Use this command to configure system administration settings, including web administration ports, timeout, and language.

Syntax

```
config system admin setting
  set access-banner {enable | disable}
  set admin-https-redirect {enable | disable}
  set admin_server_cert <admin_server_cert>
  set allow_register {enable | disable}
  set auto-update {enable | disable}
  set banner-message <string>
  set chassis-mgmt {enable | disable}
  set chassis-update-interval <integer>
  set demo-mode {enable | disable}
  set device_sync_status {enable | disable}
  set http_port <integer>
  set https_port <integer>
  set idle_timeout <integer>
  set install-ifpolicy-only {enable | disable}
  set mgmt-addr <string>
  set mgmt-fqdn <string>
  set offline_mode {enable | disable}
  set register_passwd <password_string>
  set show-add-multiple {enable | disable}
  set show-adom-central-nat-policies {enable | disable}
  set show-adom-devman {enable | disable}
  set show-adom-dos-policies {enable | disable}
  set show-adom-dynamic-objects {enable | disable}
  set show-adom-icap-policies {enable | disable}
  set show-adom-implicit-policy {enable | disable}
  set show-adom-implicit-id-based-policy {enable | disable}
  set show-adom-ipv6-settings {enable | disable}
  set show-adom-policy-consistency-button {enable | disable}
  set show-adom-rtmlog {enable | disable}
  set show-adom-sniffer-policies {enable | disable}
  set show-adom-taskmon-button {enable | disable}
  set show-adom-terminal-button {enable | disable}
  set show-adom-voip-policies {enable | disable}
  set show-adom-vpnman {enable | disable}
  set show-adom-web-portal {enable | disable}
  set show-checkbox-in-table {enable | disable}
  set show-device-import-export {enable | disable}
  set show-foc-settings {enable | disable}
```

```

set show-fortimail-settings {enable | disable}
set show-fsw-settings {enable | disable}
set show-global-object-settings {enable | disable}
set show-global-policy-settings {enable | disable}
set show_automatic_script {enable | disable}
set show_grouping_script {enable | disable}
set show_schedule_script {enable | disable}
set show_tcl_script {enable | disable}
set unreg_dev_opt {add_allow_service | add_no_service | ignore}
set webadmin_language {auto_detect | english | japanese | korean | simplified_
    chinese | traditional_chinese}
end

```

Variable	Description
access-banner {enable disable}	Enable/disable the access banner. Default: disable
admin-https-redirect {enable disable}	Enable/disable redirection of an HTTP admin traffic to HTTPS.
admin_server_cert <admin_server_ cert>	Enter the name of an HTTPS server certificate to use for secure connections. Default: server.crt
allow_register {enable disable}	Enable/disable allowing unregistered devices to be registered. Default: disable
auto-update {enable disable}	Enable/disable device config auto update.
banner-message <string>	Type the banner messages. Maximum of 255 characters. Default: none
chassis-mgmt {enable disable}	Enable/disable chassis management. Default: disable
chassis-update- interval <integer>	Set the chassis background update interval (4 - 1440 minutes). Default: 15
demo-mode {enable disable}	Enable/disable demo mode. Default: disable
device_sync_status {enable disable}	Enable/disable device synchronization status indication. Default: enable
http_port <integer>	Enter the HTTP port number for web administration. Default: 80
https_port <integer>	Enter the HTTPS port number for web administration. Default: 443
idle_timeout <integer>	Enter the idle timeout value. The range is from 1 to 480 minutes. Default: 5

Variable	Description
<code>install-ifpolicy-only {enable disable}</code>	Enable to allow only the interface policy to be installed. Default: <code>disable</code>
<code>mgmt-addr <string></code>	GQDN/IP of FortiManager used by FGFM.
<code>mgmt-fqdn <string></code>	FQDN of FortiManager used by FGFM.
<code>offline_mode {enable disable}</code>	Enable/disable offline mode to shut down the protocol used to communicate with managed devices. Default: <code>disable</code>
<code>register_passwd <password_string></code>	Enter the password to use when registering a device.
<code>show-add-multiple {enable disable}</code>	Show the add multiple button.
<code>show-adom-central-nat-policies {enable disable}</code>	Show ADOM central NAT policy settings in the GUI. Default: <code>disable</code>
<code>show-adom-devman {enable disable}</code>	Enable/disable ADOM device manager tools in the GUI. Default: <code>disable</code>
<code>show-adom-dos-policies {enable disable}</code>	Enable/disable ADOM DOS policy settings in the GUI. Default: <code>disable</code>
<code>show-adom-dynamic-objects {enable disable}</code>	Enable/disable ADOM dynamic object settings in the GUI. Default: <code>enable</code>
<code>show-adom-icap-policies {enable disable}</code>	Enable/disable the ADOMICAP policy settings in the GUI.
<code>show-adom-implicit-policy {enable disable}</code>	Enable/disable the ADOM implicit policy settings in the GUI.
<code>show-adom-implicit-id-based-policy {enable disable}</code>	Enable/disable the ADOM implicit ID based policy settings in the GUI.
<code>show-adom-ipv6-settings {enable disable}</code>	Enable/disable ADOM IPv6 settings in the GUI. Default: <code>disable</code>
<code>show-adom-policy-consistency-button {enable disable}</code>	Enable/disable ADOM banner button Policy Consistency in the GUI. Default: <code>disable</code>

Variable	Description
<code>show-adom-rtmlog {enable disable}</code>	Enable/disable ADOM RTM device log in the GUI.Default: <code>disable</code>
<code>show-adom-sniffer-policies {enable disable}</code>	Enable/disable ADOM sniffer policy settings in the GUI.Default: <code>disable</code>
<code>show-adom-taskmon-button {enable disable}</code>	Enable/disable ADOM banner button Task Monitor in the GUI. Default: <code>enable</code>
<code>show-adom-terminal-button {enable disable}</code>	Enable/disable ADOM banner button Terminal in the GUI. Default: <code>enable</code>
<code>show-adom-voip-policies {enable disable}</code>	Enable/disable ADOM VoIP policy settings in the GUI.
<code>show-adom-vpnman {enable disable}</code>	Enable/disable ADOM VPN manager in the GUI.Default: <code>enable</code>
<code>show-adom-web-portal {enable disable}</code>	Enable/disable ADOM web portal settings in the GUI.Default: <code>disable</code>
<code>show-checkbox-in-table {enable disable}</code>	Enable/disable showing checkboxes in tables in the GUI.
<code>show-device-import-export {enable disable}</code>	Enable import/export of ADOM, device, and group lists.
<code>show-foc-settings {enable disable}</code>	Enable/disable FortiCarrier settings in the GUI. Default: <code>disable</code>
<code>show-fortimail-settings {enable disable}</code>	Enable/disable FortiMail settings in the GUI. Default: <code>disable</code>
<code>show-fsw-settings {enable disable}</code>	Enable/disable FortiSwitch settings in the GUI. Default: <code>disable</code>
<code>show-global-object-settings {enable disable}</code>	Enable/disable global object settings in the GUI. Default: <code>enable</code>
<code>show-global-policy-settings {enable disable}</code>	Enable/disable global policy settings in the GUI.Default: <code>enable</code>
<code>show_automatich_script {enable disable}</code>	Enable/disable automatic script.

Variable	Description
<code>show_grouping_script</code> {enable disable}	Enable/disable grouping script.
<code>show_schedule_script</code> {enable disable}	Enable/disable schedule script.
<code>show_tcl_script</code> {enable disable}	Enable/disable TCL script.
<code>unreg_dev_opt</code> {add_ allow_service add_no_ service ignore}	Type action to take when an unregistered device connects to FortiManager. <ul style="list-style-type: none"> • <code>add_allow_service</code>: Add unregistered devices and allow service requests (default value). • <code>add_no_service</code>: Add unregistered devices and deny service requests. • <code>ignore</code>: Ignore unregistered devices.
<code>webadmin_language</code> {auto_detect english japanese korean simplified_ chinese traditional_ chinese}	Enter the language to be used for web administration. Default: <code>auto_detect</code>

admin tacacs

Use this command to add, edit, and delete administration TACACS+ servers.

Syntax

```
config system admin tacacs
edit <name>
    set authen-type <auth_prot_type>
    set authorization {enable | disable}
    set key <password_string>
    set port <integer>
    set secondary-key <password_string>
    set secondary-server <string>
    set server <string>
    set tertiary-key <password_string>
    set tertiary-server <string>
end
```

Variable	Description
<code><name></code>	Enter the name of the TACACS+ server or enter a new name to create an entry.

Variable	Description
<code>authen-type</code> <code><auth_prot_type></code>	Choose which authentication type to use. Default: <code>auto</code>
<code>authorization</code> <code>{enable disable}</code>	Enable/disable TACACS+ authorization.
<code>key</code> <code><password_string></code>	Key to access the server.
<code>port</code> <code><integer></code>	Port number of the TACACS+ server.
<code>secondary-key</code> <code><password_string></code>	Key to access the secondary server.
<code>secondary-server</code> <code><string></code>	Secondary server domain name or IP.
<code>server</code> <code><string></code>	The server domain name or IP.
<code>tertiary-key</code> <code><password_string></code>	Key to access the tertiary server.
<code>tertiary-server</code> <code><string></code>	Tertiary server domain name or IP.

Example

This example shows how to add the TACACS+ server `TAC1` at the IP address `206.205.204.203` and set the key as `R1a2D3i4U5s`.

```
config system admin tacacs
edit TAC1
set server 206.205.204.203
set key R1a2D3i4U5s
end
```

admin user

Use this command to add, edit, and delete administrator accounts.

Use the admin account or an account with System Settings read and write privileges to add new administrator accounts and control their permission levels. Each administrator account must include a minimum of an access profile. The access profile list is ordered alphabetically, capitals first. If custom profiles are defined, it may change the default profile from `Restricted_User`. You cannot delete the admin administrator account. You cannot delete an administrator account if that user is logged on.



You can create meta-data fields for administrator accounts. These objects must be created using the FortiManager GUI. The only information you can add to the object is the value of the field (pre-determined text/numbers). For more information, see *System Settings* in the FortiManager Administration Guide.

Syntax

```
config system admin user
  edit <name_str>
    set password <password_string>
    set change-password {enable | disable}
    set trusthost1 <ipv4_mask>
    set trusthost2 <ipv4_mask>
    set trusthost3 <ipv4_mask>
    ...
    set trusthost10 <ipv4_mask>
    set ipv6_trusthost1 <ipv6_mask>
    set ipv6_trusthost2 <ipv6_mask>
    set ipv6_trusthost3 <ipv6_mask>
    ...
    set ipv6_trusthost10 <ipv6_mask>
    set profileid <profile-name>
    set adom <adom_name(s)>
    set web-filter <Web Filter profile name>
    set ips-filter <IPS Sensor name>
    set app-filter <Application Sensor name>
    set policy-package {<adom name>: <policy package id> <adom policy folder name>/
    <package name> | all_policy_packages}
    set restrict-access {enable | disable}
    set description <string>
    set user_type <group | ldap | local | pki-auth | radius | tacacs-plus>
    set set_group <string>
    set ldap-server <string>
    set radius_server <string>
    set tacacs-plus-server <string>
    set ssh-public-key1 <key-type> <key-value>
    set ssh-public-key2 <key-type>, <key-value>
    set ssh-public-key3 <key-type> <key-value>
    set wildcard {enable | disable}
    set radius-accpfile-override {enable | disable}
    set radius-adom-override {enable | disable}
    set radius-group-match <string>
    set password-expire <yyyy-mm-dd>
    set force-password-change {enable | disable}
    set subject <string>
    set ca <string>
    set two-factor-auth {enable | disable}
    set last-name <string>
    set first-name <string>
    set email-address <string>
    set phone-number <string>
    set mobile-number <string>
    set pager-number <string>
  end
config meta-data
  edit <fieldname>
```

```

        set fieldlength
        set fieldvalue <string>
        set importance
        set status
    end
end
config dashboard-tabs
    edit tabid <integer>
        set name <string>
    end
end
config dashboard
    edit moduleid
        set name <string>
        set column <column_position>
        set refresh-interval <integer>
        set status {close | open}
        set tabid <integer>
        set widget-type <string>
        set log-rate-type {device | log}
        set log-rate-topn {1 | 2 | 3 | 4 | 5}
        set log-rate-period {1hour | 2min | 6hours}
        set res-view-type {history | real-time}
        set res-period {10min | day | hour}
        set res-cpu-display {average | each}
        set num-entries <integer>
        set time-period <integer>
    end
end
config restrict-dev-vdom
    edit dev-vdom <string>
end
end
end

```

Variable	Description
password <password_string>	Enter a password for the administrator account. For improved security, the password should be at least 6 characters long. This variable is available only if <code>user_type</code> is <code>local</code> .
change-password {enable disable}	Enable/disable allowing the admin user to change their password.
trusthost1 <ipv4_mask> trusthost2 <ipv4_mask> trusthost3 <ipv4_mask> ... trusthost10 <ipv4_mask>	<p>Optionally, type the trusted host IPv4 address and network mask from which the administrator can log in to the FortiManager system. You can specify up to ten trusted hosts. Setting trusted hosts for all of your administrators can enhance the security of your system.</p> <p>Defaults:</p> <ul style="list-style-type: none"> • <code>trusthost1: 0.0.0.0 0.0.0.0</code> for all • <code>others: 255.255.255.255 255.255.255.255</code> for none

Variable	Description
<pre> ipv6_trusthost1 <ipv6_ mask> ipv6_trusthost2 <ipv6_ mask> ipv6_trusthost3 <ipv6_ mask> ... ipv6_trusthost10 <ipv6_mask> </pre>	<p>Optionally, type the trusted host IPv6 address from which the administrator can log in to the FortiManager system. You can specify up to ten trusted hosts.</p> <p>Setting trusted hosts for all of your administrators can enhance the security of your system.</p> <p>Defaults:</p> <ul style="list-style-type: none"> • <code>ipv6_trusthost1: ::/0</code> for all • others: <code>ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128</code> for none
<pre> profileid <profile- name> </pre>	<p>Enter the name of the access profile to assign to this administrator account. Access profiles control administrator access to FortiManager features. Default: <code>Restricted_User</code></p>
<pre> adom <adom_name(s)> </pre>	<p>Enter the name(s) of the ADOM(s) the administrator belongs to. Any configuration of ADOMs takes place via the FortiManager GUI.</p>
<pre> web-filter <Web Filter profile name> </pre>	<p>Enter the Web Filter profile to associate with the restricted admin profile.</p> <p>Dependencies: The admin user must be associated with a restricted admin profile.</p>
<pre> ips-filter <IPS Sensor name> </pre>	<p>Enter the IPS Sensor to associate with the restricted admin profile.</p> <p>Dependencies: The admin user must be associated with a restricted admin profile.</p>
<pre> app-filter <Application Sensor name> </pre>	<p>Enter the Application Sensor to associate with the restricted admin profile.</p> <p>Dependencies: The admin user must be associated with a restricted admin profile.</p>
<pre> policy-package {<adom name>: <policy package id> <adom policy folde r name>/ <package name> all_policy_ packages} </pre>	<p>Policy package access</p>
<pre> restrict-access {enable disable} </pre>	<p>Enable/disable restricted access to the development VDOM (<code>dev-vdom</code>). Default: <code>disable</code></p>
<pre> description <string> </pre>	<p>Enter a description for this administrator account. When using spaces, enclose description in quotes.</p>

Variable	Description
<code>user_type <group ldap local pki-auth radius tacacs-plus></code>	Enter <code>local</code> if the FortiManager system verifies the administrator's password. Enter <code>radius</code> if a RADIUS server verifies the administrator's password. Default: <code>local</code>
<code>set group <string></code>	Enter the group name.
<code>ldap-server <string></code>	Enter the LDAP server name if the user type is set to LDAP.
<code>radius_server <string></code>	Enter the RADIUS server name if the user type is set to RADIUS.
<code>tacacs-plus-server <string></code>	Enter the TACACS+ server name if the user type is set to TACACS+.
<code>ssh-public-key1 <key-type> <key-value></code> <code>ssh-public-key2 <key-type>, <key-value></code> <code>ssh-public-key3 <key-type> <key-value></code>	You can specify the public keys of up to three SSH clients. These clients are authenticated without being asked for the administrator password. You must create the public-private key pair in the SSH client application. <ul style="list-style-type: none"> <code><key type></code> is <code>ssh-dss</code> for a DSA key, <code>ssh-rsa</code> for an RSA key. <code><key-value></code> is the public key string of the SSH client.
<code>wildcard <enable disable></code>	Enable/disable wildcard remote authentication
<code>radius-accprofile-override <enable disable></code>	Enable/disable allowing the access profile to be overridden from RADIUS.
<code>radius-adom-override <enable disable></code>	Enable/disable allowing the ADOM to be overridden from RADIUS
<code>radius-group-match <string></code>	Only admin that belong to this group are allowed to log in.
<code>password-expire <yyyy-mm-dd></code>	When enforcing the password policy, enter the date that the current password will expire.
<code>force-password-change {enable disable}</code>	Enable/disable force password change on next login.
<code>subject <string></code>	PKI user certificate name constraints. This command is available when a PKI administrator account is configured.
<code>ca <string></code>	PKI user certificate CA (CA name in local). This command is available when a PKI administrator account is configured.

Variable	Description
two-factor-auth {enable disable}	Enable/disable two-factor authentication (certificate + password). This command is available when a PKI administrator account is configured.
last-name <string>	Administrators last name.
first-name <string>	Administrators first name.
email-address <string>	Administrators email address.
phone-number <string>	Administrators phone number.
mobile-number <string>	Administrators mobile phone number.
pager-number <string>	Administrators pager number.
Variables for config meta-data subcommand: This subcommand can only change the value of an existing field. To create a new metadata field, use the config meta-data command.	
fieldname	The label/name of the field. Read-only. Default: 50
fieldlength	The maximum number of characters allowed for this field. Read-only.
fieldvalue <string>	Enter a pre-determined value for the field. This is the only value that can be changed with the config meta-data subcommand.
importance	Indicates whether the field is compulsory (required) or optional (optional). Read-only. Default: optional
status	For display only. Value cannot be changed. Default: enable
Variable for config dashboard-tabs subcommand:	
tabid <integer>	Tab ID.
name <string>	Tab name.
Variable for config dashboard subcommand:	

Variable	Description
<code>moduleid</code>	Widget ID. 1: System Information 2: System Resources 3: License Information 4: Unit Operation 5: Alert Message Console 6: CLI Console 7: Log Receive Monitor 8: Statistics 9: Logs/Data Received
<code>name <string></code>	Widget name.
<code>column <column_ position></code>	Widget's column ID. Default: 0
<code>refresh-interval <integer></code>	Widget's refresh interval.Default: 300
<code>status {close open}</code>	Widget's opened/closed status.Default: open
<code>tabid <integer></code>	ID of the tab where the widget is displayed.Default: 0
<code>widget-type <string></code>	Widget type.
<code>log-rate-type {device log}</code>	Log receive monitor widget's statistics breakdown options.
<code>log-rate-topn {1 2 3 4 5}</code>	Log receive monitor widgets's number of top items to display.
<code>log-rate-period {1hour 2min 6hours}</code>	Log receive monitor widget's data period.
<code>res-view-type {history real-time}</code>	Widget's data view type.
<code>res-period {10min day hour}</code>	Widget's data period.
<code>res-cpu-display {average each}</code>	Widget's CPU display type.

Variable	Description
num-entries <integer>	Number of entries.
time-period <integer>	Time period
Variable for <code>config restrict-dev-vdom</code> subcommand:	
dev-vdom <string>	Enter device or VDOM to edit.

Using trusted hosts

Setting trusted hosts for all of your administrators increases the security of your network by further restricting administrative access. In addition to knowing the password, an administrator must connect only through the subnet or subnets you specify. You can even restrict an administrator to a single IP address if you define only one trusted host IP address with a netmask of 255.255.255.255.

When you set trusted hosts for all administrators, the FortiManager system does not respond to administrative access attempts from any other hosts. This provides the highest security. If you leave even one administrator unrestricted, the unit accepts administrative access attempts on any interface that has administrative access enabled, potentially exposing the unit to attempts to gain unauthorized access.

The trusted hosts you define apply both to the GUI and to the CLI when accessed through SSH. CLI access through the console connector is not affected.

Example

Use the following commands to add a new administrator account named `admin_2` with the password set to `p8ssw0rd` and the `Super_User` access profile. Administrators that log in to this account will have administrator access to the FortiManager system from any IP address.

```
config system admin user
  edit admin_2
    set description "Backup administrator"
    set password p8ssw0rd
    set profileid Super_User
  end
```

alert-console

Use this command to configure the alert console options. The alert console appears on the dashboard in the GUI.

Syntax

```
config system alert-console
  set period <integer>
  set severity-level {information | notify | warning | error | critical | alert |
  emergency}
end
```

Variable	Description
period <integer>	Enter the number of days to keep the alert console information on the dashboard in days between 1 and 7. Default: 7
severity-level {information notify warning error critical alert emergency}	Enter the severity level to display on the alert console on the dashboard.

Example

This example sets the alert console message display to warning for a duration of three days.

```
config system alert-console
  set period 3
  set severity-level warning
end
```

alert-event

Use `alert-event` commands to configure the FortiManager unit to monitor logs for log messages with certain severity levels, or information within the logs. If the message appears in the logs, the FortiManager unit sends an email or SNMP trap to a predefined recipient(s) of the log message encountered. Alert event messages provide immediate notification of issues occurring on the FortiManager unit.

When configuring an alert email, you must configure at least one DNS server. The FortiGate unit uses the SMTP server name to connect to the mail server and must look up this name on your DNS server.



`alert-event` was removed from the GUI in version 5.0.3. This command has been kept in the CLI for customers who previously configured this function.

Syntax

```
config system alert-event
  edit <name_string>
  config alert-destination
    edit destination_id <integer>
      set type {mail | snmp | syslog}
      set from <email_address>
      set to <email_addr>
      set smtp-name <server_name>
      set snmp-name <server_name>
      set syslog-name <server_name>
    end
    set enable-generic-text {enable | disable}
    set enable-severity-filter {enable | disable}
    set event-time-period {0.5 | 1 | 3 | 6 | 12 | 24 | 72 | 168}
    set generic-text <string>
```

```

set num-events {1 | 5 | 10 | 50 | 100}
set severity-filter {high | low | medium | medium-high | medium-low}
set severity-level-comp {>= | = | <=}
set severity-level-logs {no-check | information | notify | warning | error |
critical | alert | emergency}
end

```

Variable	Description
<name_string>	Enter a name for the alert event.
destination_id <integer>	Enter the table sequence number, beginning at 1.
type {mail snmp syslog}	Type the alert event message method of delivery. Default: mail
from <email_ address>	Enter the email address of the sender of the message. This is available when the type is set to mail.
to <email_addr>	Enter the recipient of the alert message. This is available when the type is set to mail.
smtp-name <server_ name>	Enter the name of the mail server. This is available when the type is set to mail.
snmp-name <server_ name>	Enter the snmp server name. This is available when the type is set to snmp.
syslog-name <server_ name>	Enter the syslog server name or IP address. This is available when the type is set to syslog.
enable-generic-text {enable disable}	Enable/disable the text alert option. Default: disable
enable-severity-filter {enable disable}	Enable/disable the severity filter option. Default: disable
event-time-period {0.5 1 3 6 12 24 72 168}	The period of time in hours during which if the threshold number is exceeded, the event will be reported.
generic-text <string>	Enter the text the alert looks for in the log messages.

Variable	Description
num-events {1 5 10 50 100}	Set the number of events that must occur in the given interval before it is reported.
severity-filter {high low medium medium-high medium-low}	Set the alert severity indicator for the alert message the FortiManager unit sends to the recipient.
severity-level-comp {>= = <=}	Set the severity level in relation to the log level. Log messages are monitored based on the log level. For example, alerts may be monitored if the messages are greater than, and equal to (>=) the Warning log level.
severity-level-logs {no-check information notify warning error critical alert emergency}	Set the log level the FortiManager looks for when monitoring for alert messages.

Example

In the following example, the alert message is set to send an email to the administrator when 5 warning log messages appear over the span of three hours.

```
config system alert-event
  edit warning
    config alert-destination
      edit 1
        set type mail
        set from fmgr@example.com
        set to admin@example.com
        set smtp-name mail.example.com
      end
    set enable-severity-filter enable
    set event-time-period 3
    set severity-level-log warning
    set severity-level-comp =
    set severity-filter medium
  end
```

alertemail

Use this command to configure alert email settings for your FortiManager unit.

All variables are required if `authentication` is enabled.

Syntax

```
config system alertemail
  set authentication {enable | disable}
  set fromaddress <email-addr_string>
  set fromname <name_string>
  set smtppassword <password_string>
  set smtpport <port_int>
  set smtpserver {<ipv4>|<fqdn_string>}
  set smtpuser <username_string>
end
```

Variable	Description
authentication {enable disable}	Enable/disable alert email authentication.Default: enable
fromaddress <email-addr_string>	The email address the alertmessage is from.This is a required variable.
fromname <name_string>	The SMTP name associated with the email address. To enter a name that includes spaces, enclose the whole name in quotes.
smtppassword <password_string>	Set the SMTP server password.
smtpport <port_int>	The SMTP server port.Default: 25
smtpserver {<ipv4> <fqdn_string>}	The SMTP server address. Enter either a DNS resolvable host name or an IPv4 address.
smtpuser <username_string>	Set the SMTP server username.

Example

Here is an example of configuring `alertemail`. Enable authentication, the alert is set in Mr. Customer's name and from his email address, the SMTP server port is the default port(25), and the SMTP server is at IP address of 192.168.10.10.

```
config system alertemail
  set authentication enable
  set fromaddress customer@example.com
  set fromname "Mr. Customer"
  set smtpport 25
  set smtpserver 192.168.10.10
end
```

auto-delete

Use this command to automatically delete policies for logs, reports, and archived and quarantined files.

Syntax

```

config system auto-delete
  config dlp-files-auto-deletion
    set status {enable | disable}
    set value <integer>
    set when {days | hours | months | weeks}
  end
  config quarantine-files-auto-deletion
    set status {enable | disable}
    set value <integer>
    set when {days | hours | months | weeks}
  end
  config log-auto-deletion
    set status {enable | disable}
    set value <integer>
    set when {days | hours | months | weeks}
  end
  config report-auto-deletion
    set status {enable | disable}
    set value <integer>
    set when {days | hours | months | weeks}
  end
end

```

Variable	Description
dlp-files-auto-deletion	Automatic deletion policy for DLP archives.
quarantine-files-auto-deletion	Automatic deletion policy for quarantined files.
log-auto-deletion	Automatic deletion policy for device logs.
report-auto-deletion	Automatic deletion policy for reports.
status {enable disable}	Enable/disable automatic deletion.
value <integer>	Set the value integer.
when {days hours months weeks}	Auto-delete data older that <value> days, hours, months, weeks.

backup all-settings

Use this command to set or check the settings for scheduled backups.

Syntax

```

config system backup all-settings
    set status {enable | disable}
    set server {<ipv4>|<fqdn_str>}
    set user <username_string>
    set directory <dir_str>
    set week_days {monday tuesday wednesday thursday friday saturday sunday}
    set time <hh:mm:ss>
    set protocol {ftp | scp | sftp}
    set passwd <password_string>
    set cert <string>
    set crptpasswd <password_string>
end

```

Variable	Description
status {enable disable}	Enable/disable scheduled backups. Default: disable
server {<ipv4> <fqdn_str>}	Enter the IPv4 address or DNS resolvable host name of the backup server.
user <username_string>	Enter the user account name for the backup server.
directory <dir_str>	Enter the name of the directory on the backup server in which to save the backup file.
week_days {monday tuesday wednesday thursday friday saturday sunday}	Enter days of the week on which to perform backups. You may enter multiple days.
time <hh:mm:ss>	Enter time of day to perform the backup. Time is required in the form <hh:mm:ss>.
protocol {ftp scp sftp}	Enter the transfer protocol. Default: sftp
passwd <password_string>	Enter the password for the backup server.
cert <string>	SSH certificate for authentication. Only available if the protocol is set to scp.
crptpasswd <password_string>	Optional password to protect backup content

Example

This example shows a whack where backup server is 172.20.120.11 using the admin account with no password, saving to the /usr/local/backup directory. Backups are done on Mondays at 1:00pm using ftp.

```
config system backup all-settings
    set status enable
    set server 172.20.120.11
    set user admin
    set directory /usr/local/backup
    set week_days monday
    set time 13:00:00
    set protocol ftp
end
```

certificate

Use the following commands to configure certificate related settings.

certificate ca

Use this command to install Certificate Authority (CA) root certificates.

When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA.

The CA sends you the CA certificate, the signed local certificate and the CRL.

3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate.

Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate ca
    edit <ca_name>
        set ca <cert>
        set comment <string>
    end
```

To view all of the information about the certificate, use the `get` command:

```
get system certificate ca <ca_name>
```

Variable	Description
<ca_name>	Enter a name for the CA certificate.

Variable	Description
ca <cert>	Enter or retrieve the CA certificate in PEM format.
comment <string>	Optionally, enter a descriptive comment.

certificate crl

Use this command to configure CRLs.

Syntax

```
config system certificate crl
  edit <name>
    set crl <crl>
    set comment <string>
  end
```

Variable	Description
<name>	Enter a name for the CRL.
crl <crl>	Enter or retrieve the CRL in PEM format.
comment <string>	Optionally, enter a descriptive comment for this CRL.

certificate local

Use this command to install local certificates. When a CA processes your CSR, it sends you the CA certificate, the signed local certificate and the CRL.

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA.
The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate.
Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate local
  edit <cert_name>
    set password <cert_password>
    set comment <comment_text>
    set certificate <cert_PEM>
    set private-key <prkey>
    set csr <csr_PEM>
  end
```

To view all of the information about the certificate, use the `get` command:

```
get system certificate local [cert_name]
```

Variable	Description
<cert_name>	Enter the local certificate name.
password <cert_ password>	Enter the local certificate password.
comment <comment_ text>	Enter any relevant information about the certificate.
certificate <cert_PEM>	Enter the signed local certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit.	
private-key <prkey>	The private key in PEM format.
csr <csr_PEM>	The CSR in PEM format.

certificate oftp

Use this command to install OFTP certificates and keys.

Syntax

```
config system certificate oftp
    set certificate <certificate>
    set comment <string>
    set custom {enable | disable}
    set private-key <key>
end
```

Variable	Description
certificate <certificate>	PEM format certificate.
comment <string>	OFTP certificate comment.
custom {enable disable}	Enable/disable custom certificates
private-key <key>	PEM format private key.

certificate ssh

Use this command to install SSH certificates and keys.

The process for obtaining and installing certificates is as follows:

1. Use the `execute certificate local generate` command to generate a CSR.
2. Send the CSR to a CA.

The CA sends you the CA certificate, the signed local certificate and the CRL.

3. Use the `system certificate local` command to install the signed local certificate.
4. Use the `system certificate ca` command to install the CA certificate.
5. Use the `system certificate SSH` command to install the SSH certificate.

Depending on your terminal software, you can copy the certificate and paste it into the command.

Syntax

```
config system certificate ssh
  edit <name>
    set comment <comment_text>
    set certificate <certificate>
    set private-key <key>
  end
```

To view all of the information about the certificate, use the `get` command:

```
get system certificate ssh [cert_name]
```

Variable	Description
<name>	Enter the SSH certificate name.
comment <comment_text>	Enter any relevant information about the certificate.
certificate <certificate>	Enter the signed SSH certificate in PEM format.
You should not modify the following variables if you generated the CSR on this unit.	
private-key <key>	The private key in PEM format.

dm

Use this command to configure Deployment Manager (DM) settings.

Syntax

```
config system dm
  set concurrent-install-limit <installs_int>
  set concurrent-install-script-limit <scripts_int>
  set discover-timeout <integer>
  set dpm-logsize <kbytes_int>
  set fgfm-sock-timeout <sec_int>
  set fgfm_keepalive_itvl <sec_int>
  set force-remote-diff {enable | disable}
  set max-revs <revs_int>
  set nr-retry <retries_int>
```

```

set retry {enable | disable}
set retry-intvl <sec_int>
set rollback-allow-reboot {enable | disable}
set script-logsize <integer>
set verify-install {enable | disable}
set fortiap-refresh-itvl <integer>
end

```

Variable	Description
concurrent-install-limit <installs_int>	The maximum number of concurrent installs. The range can be from 5 to 100. Default: 60
concurrent-install-script-limit <scripts_int>	The maximum number of concurrent install scripts. The range can be from 5 to 100. Default: 60
discover-timeout <integer>	Check connection timeout when discovering a device (3-15).
dpm-logsize <kbytes_int>	The maximum DPM log size per device in kB. The range can be from 1 to 10000kB. Default: 10000
fgfm-sock-timeout <sec_int>	The maximum FortiManager/FortiGate communication socket idle time. The interval can be from 90 to 1800 seconds. Default: 900
fgfm-keepalive-itvl <sec_int>	The interval at which the FortiManager will send a keepalive signal to a FortiGate unit to keep the FortiManager/FortiGate communication protocol active. The interval can be from 30 to 600 seconds. Default: 300
force-remote-diff {enable disable}	Enable to always use remote diff when installing. Default: disable
max-revs <revs_int>	The maximum number of revisions saved. Valid numbers are from 1 to 250. Default: 100
nr-retry <retries_int>	The number of times the FortiManager unit will retry. Default: 1
retry {enable disable}	Enable/disable configuration installation retries. Default: enable
retry-intvl <sec_int>	The interval between attempting another configuration installation following a failed attempt. Default: 15
rollback-allow-reboot {enable disable}	Enable to allow a FortiGate unit to reboot when installing a script or configuration. Default: disable
script-logsize <integer>	Enter the maximum script log size per device (1-10000kB).

Variable	Description
verify-install {enable disable}	Enable to verify install against remote configuration. Default: enable
fortiap-refresh-itvl <integer>	Set the auto refresh FortiAP status interval, from 1-1440 minutes.

Example

This example shows how to set up configuration installations. It shows how to set 5 attempts to install a configuration on a FortiGate device, waiting 30 seconds between attempts.

```
config system dm
  set retry enable
  set nr-retry 5
  set retry-intvl 30
end
```

dns

Use this command to set the DNS server addresses. Several FortiManager functions, including sending alert email, use DNS.

Syntax

```
config system dns
  set primary <ipv4_address>
  set secondary <ipv4_address>
end
```

Variable	Description
primary <ipv4_address>	Enter the primary DNS server IPv4 address.
secondary <ipv4_address>	Enter the secondary DNS IPv4 server address.

Example

This example shows how to set the primary FortiManager DNS server IP address to 172.20.120.99 and the secondary FortiManager DNS server IP address to 192.168.1.199.

```
config system dns
  set primary 172.20.120.99
  set secondary 192.168.1.199
end
```

fips

Use this command to set the Federal Information Processing Standards (FIPS) status. FIPS mode is an enhanced security option for some FortiManager models. Installation of FIPS firmware is required only if the unit was not ordered with this firmware pre-installed.

Syntax

```
config system fips
  set status {enable | disable}
  set fortitrng {enable | disable} | dynamic]
  set re-seed-interval <integer>
end
```

Variable	Description	Default
status {enable disable}	Enable/disable the FIPS-CC mode of operation.	enable
fortitrng {enable disable} dynamic]	Configure support for the FortiTRNG entropy token: <ul style="list-style-type: none"> enable: The token must be present during boot up and reseeding. If the token is not present, the boot up or reseeding is interrupted until the token is inserted. disable: The current entropy implementation is used to seed the Random Number Generator (RNG). dynamic: The token is used to seed or reseed the RNG if it is present. If the token is not present, the boot process is not blocked and the old entropy implementation is used. 	disable
re-seed-interval <integer>	The amount of time, in minutes, between RNG reseeding.	1440

global

Use this command to configure global settings that affect miscellaneous FortiManager features.

Syntax

```
config system global
  set admin-https-pki-required {disable | enable}
  set admin-lockout-duration <integer>
  set admin-lockout-threshold <integer>
  set admin-maintainer {disable | enable}
  set admintimeout <integer>
  set adom-mode {advanced | normal}sh
  set adom-rev-auto-delete {by-days | by-revisions | disable}
  set adom-rev-max-days <integer>
  set adom-rev-max-revisions <integer>
  set adom-status {enable | disable}
  set clt-cert-req {disable | enable}
```

```

set console-output {more | standard}
set daylightsavetime {enable | disable}
set default-disk-quota <integer>
set dh-params < >
set faz-status {enable | disable}
set enc-algorithm {default | high | low}
set hostname <string>
set language {english | japanese | simch | trach}
set ldapconntimeout <integer>
set lcdpin <integer>
set lock-preempt {enable | disable}
set log-checksum {md5 | md5-auth | none}
set max-concurrent-users <integer>
set max-running-reports <integer>
set partial-install {enable | disable}
set unregister-pop-up {enable | disable}
set pre-login-banner {disable | enable}
set pre-login-banner-message <string>
set remoteauthtimeout <integer>
set search-all-adoms {enable | disable}
set ssl-low-encryption {enable | disable}
set ssl-protocol {tlsv1 | sslv3}
set swapmem {enable | disable}
set task-list-size <integer>
set timezone <timezone_int>
set vdom-mirror {enable | disable}
set webservice-proto {tlsv1 | sslv3 | sslv2}
set workspace-mode {disabled | normal | workflow}
end

```

Variable	Description
admin-https-pki-required {disable enable}	Enable/disable HTTPS login page when PKI is enabled.
admin-lockout-duration <integer>	Set the lockout duration (seconds) for FortiManager administration. Default: 60
admin-lockout-threshold <integer>	Set the lockout threshold for FortiManager administration (1 to 10). Default: 3
admin-maintainer {disable enable}	Enable/disable the special user maintainer account.
admintimeout <integer>	Set the administrator idle timeout (in minutes). Default: 5
adom-mode {advanced normal}	Set the ADOM mode.
adom-rev-auto-delete {by-days by-revisions disable}	Auto delete features for old ADOM revisions.

Variable	Description
adom-rev-max-days <integer>	The maximum number of days to keep old ADOM revisions.
adom-rev-max-revisions <integer>	The maximum number of ADOM revisions to keep.
adom-status {enable disable}	Enable/disable administrative domains (ADOMs). Default: disable
clt-cert-req {disable enable}	Enable/disable requiring a client certificate for GUI login.
console-output {more standard}	Select how the output is displayed on the console. Type <code>more</code> to pause the output at each full screen until keypress. Type <code>standard</code> for continuous output without pauses. Default: standard
daylightsavetime {enable disable}	Enable/disable daylight saving time. If you enable daylight saving time, the FortiManager unit automatically adjusts the system time when daylight saving time begins or ends. Default: enable
default-disk-quota <integer>	Default disk quota (MB) for registered device.
faz-status {enable disable}	Enable/disable FortiAnalyzer status. Note: This command is not available on the FMG-100C.
enc-algorithm {default high low}	Set SSL communication encryption algorithms. Default: default
hostname <string>	FortiManager host name.
language {english japanese simch trach}	GUI language. Type one of the following: <ul style="list-style-type: none"> english: English japanese: Japanese simch: Simplified Chinese trach: Traditional Chinese Default: English
ldapconntimeout <integer>	LDAP connection timeout (in milliseconds). Default: 60000
lcdpin <integer>	Set the 6-digit PIN administrators must enter to use the LCD panel.
lock-preempt {enable disable}	Enable/disable the ADOM lock override.

Variable	Description
<code>log-checksum {md5 md5-auth none}</code>	Record log file hash value, timestamp, and authentication code at transmission or rolling. Select one of the following: <ul style="list-style-type: none"> <code>md5</code>: Record log file's MD5 hash value only <code>md5-auth</code>: Record log file's MD5 hash value and authentication code <code>none</code>: Do not record the log file checksum
<code>max-concurrent-users <integer></code>	Maximum number of concurrent administrators.Default: 20
<code>max-running-reports <integer></code>	Maximum running reports number. (Min:1, Max: 10)
<code>partial-install {enable disable}</code>	Enable/disable partial install (install only some objects). Use this command to enable pushing individual objects of the policy package down to all FortiGates in the Policy Package. Once enabled, in the GUI you can right-click an object and choose to install it.
<code>unregister-pop-up {enable disable}</code>	Enable/disable unregistered device popup messages in the GUI.
<code>pre-login-banner {disable enable}</code>	Enable/disable pre-login banner.
<code>pre-login-banner-message <string></code>	Set the pre-login banner message.
<code>remoteauthtimeout <integer></code>	Remote authentication (RADIUS/LDAP) timeout (in seconds). Default: 10
<code>search-all-adoms {enable disable}</code>	Enable/disable search all ADOMs for where-used queries.
<code>ssl-low-encryption {enable disable}</code>	Enable/disable low-grade (40-bit) encryption.Default: enable
<code>ssl-protocol {tlsv1 sslv3}</code>	Set the SSL protocols. <ul style="list-style-type: none"> <code>tlsv1</code>: Enable TLSv1 <code>sslv3</code>: Enable SSLv3
<code>swapmem {enable disable}</code>	Enable/disable virtual memory.
<code>task-list-size <integer></code>	Set the maximum number of completed tasks to keep. The default task list size is 2000.
<code>timezone <timezone_int></code>	The time zone for the FortiManager unit.Default: (GMT-8) Pacific Time(US & Canada)

Variable	Description
<pre>vdom-mirror {enable disable}</pre>	<p>Enable/disable VDOM mirror. Once enabled in the CLI, you can select to enable VDOM Mirror when editing a virtual domain in the <i>System > Virtual Domain</i> device tab in Device Manager. You can then add devices and VDOMs to the list so they may be mirrored. A icon is displayed in the Mirror column of this page to indicate that the VDOM is being mirrored to another device/VDOM. When changes are made to the master device's VDOM database, a copy is applied to the mirror device's VDOM database. A revision is created and then installed to the devices.</p> <p>Default: <code>disabled</code></p> <p>Note: VDOM mirror is intended to be used by MSSP or enterprise companies who need to provide a backup VDOM for their customers.</p>
<pre>webservice-proto {tls1 sslv3 sslv2}</pre>	<p>WebService connection using one of the following protocols:</p> <ul style="list-style-type: none"> • <code>tls1</code>: TLSv1 protocol • <code>sslv3</code>: SSLv3 protocol • <code>sslv2</code>: SSLv2 protocol
<pre>workspace-mode {disabled normal workflow}</pre>	<p>Enable/disable Workspace and Workflow (ADOM locking). Select one of the following options:</p> <ul style="list-style-type: none"> • <code>disabled</code>: Workspace is disabled. • <code>normal</code>: Workspace lock mode enabled. • <code>workspace</code>: Workspace workflow mode enabled.

Example

The following command turns on daylight saving time, sets the FortiManager unit name to FMG3k, and chooses the Eastern time zone for US & Canada.

```
config system global
    set daylightsavetime enable
    set hostname FMG3k
    set timezone 12
end
```

Integer	Time zone	Integer	Time zone
00	(GMT-12:00) Eniwetak, Kwajalein	41	(GMT+3:30) Tehran
01	(GMT-11:00) Midway Island, Samoa	42	(GMT+4:00) Abu Dhabi, Muscat
02	(GMT-10:00) Hawaii	43	(GMT+4:00) Baku
03	(GMT-9:00) Alaska	44	(GMT+4:30) Kabul
04	(GMT-8:00) Pacific Time (US & Canada)	45	(GMT+5:00) Ekaterinburg
05	(GMT-7:00) Arizona	46	(GMT+5:00) Islamabad, Karachi, Tashkent

Integer	Time zone	Integer	Time zone
06	(GMT-7:00) Mountain Time (US & Canada)	47	(GMT+5:30) Calcutta, Chennai, Mumbai, New Delhi
07	(GMT-6:00) Central America	48	(GMT+5:45) Kathmandu
08	(GMT-6:00) Central Time (US & Canada)	49	(GMT+6:00) Almaty, Novosibirsk
09	(GMT-6:00) Mexico City	50	(GMT+6:00) Astana, Dhaka
10	(GMT-6:00) Saskatchewan	51	(GMT+6:00) Sri Jayawardenapura
11	(GMT-5:00) Bogota, Lima, Quito	52	(GMT+6:30) Rangoon
12	(GMT-5:00) Eastern Time (US & Canada)	53	(GMT+7:00) Bangkok, Hanoi, Jakarta
13	(GMT-5:00) Indiana (East)	54	(GMT+7:00) Krasnoyarsk
14	(GMT-4:00) Atlantic Time (Canada)	55	(GMT+8:00) Beijing, ChongQing, HongKong, Urumqi
15	(GMT-4:00) La Paz	56	(GMT+8:00) Irkutsk, Ulaanbaatar
16	(GMT-4:00) Santiago	57	(GMT+8:00) Kuala Lumpur, Singapore
17	(GMT-3:30) Newfoundland	58	(GMT+8:00) Perth
18	(GMT-3:00) Brasilia	59	(GMT+8:00) Taipei
19	(GMT-3:00) Buenos Aires, Georgetown	60	(GMT+9:00) Osaka, Sapporo, Tokyo, Seoul
20	(GMT-3:00) Nuuk (Greenland)	61	(GMT+9:00) Yakutsk
21	(GMT-2:00) Mid-Atlantic	62	(GMT+9:30) Adelaide
22	(GMT-1:00) Azores	63	(GMT+9:30) Darwin
23	(GMT-1:00) Cape Verde Is	64	(GMT+10:00) Brisbane
24	(GMT) Casablanca, Monrovia	65	(GMT+10:00) Canberra, Melbourne, Sydney
25	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London	66	(GMT+10:00) Guam, Port Moresby
26	(GMT+1:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna	67	(GMT+10:00) Hobart

Integer	Time zone	Integer	Time zone
27	(GMT+1:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague	68	(GMT+10:00) Vladivostok
28	(GMT+1:00) Brussels, Copenhagen, Madrid, Paris	69	(GMT+11:00) Magadan
29	(GMT+1:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb	70	(GMT+11:00) Solomon Is., New Caledonia
30	(GMT+1:00) West Central Africa	71	(GMT+12:00) Auckland, Wellington
31	(GMT+2:00) Athens, Istanbul, Minsk	72	(GMT+12:00) Fiji, Kamchatka, Marshall Is
32	(GMT+2:00) Bucharest	73	(GMT+13:00) Nuku'alofa
33	(GMT+2:00) Cairo	74	(GMT-4:30) Caracas
34	(GMT+2:00) Harare, Pretoria	75	(GMT+1:00) Namibia
35	(GMT+2:00) Helsinki, Riga, Tallinn	76	(GMT-5:00) Brazil-Acre)
36	(GMT+2:00) Jerusalem	77	(GMT-4:00) Brazil-West
37	(GMT+3:00) Baghdad	78	(GMT-3:00) Brazil-East
38	(GMT+3:00) Kuwait, Riyadh	79	(GMT-2:00) Brazil-DeNoronha
39	(GMT+3:00) Moscow, St.Petersburg, Volgograd		
40	(GMT+3:00) Nairobi		

ha

Use the `config system ha` command to enable and configure FortiManager high availability (HA). FortiManager HA provides a solution for a key requirement of critical enterprise management and networking components: enhanced reliability.

A FortiManager HA cluster consists of up five FortiManager units of the same FortiManager model. One of the FortiManager units in the cluster operates as a primary or master unit and the other one to four units operate as backup units. All of the units are visible on the network. The primary unit and the backup units can be at the same location. FortiManager HA also supports geographic redundancy so the primary unit and backup units can be in different locations attached to different networks as long as communication is possible between them (for example over the Internet, over a WAN, or through a private network).

Administrators connect to the primary unit GUI or CLI to perform FortiManager operations. The primary unit also interacts with managed FortiGate devices, and FortiSwitch devices. Managed devices connect with the primary

unit for configuration backup and restore. If FortiManager is being used to distribute firmware updates and FortiGuard updates to managed devices, the managed devices can connect to the primary unit or one of the backup units.

If the primary FortiManager unit fails you must manually configure one of the backup units to become the primary unit. The new primary unit will have the same IP addresses as it did when it was the backup unit. For the managed devices to automatically start using the new primary unit, you should add all of the FortiManager units in the cluster to the managed devices.

To configure a cluster, use the `config system ha` command to set the HA operation mode (`mode`) to `ha` and set the local IP1 (`local-ip1`), peer IP1 (`peer-ip1`) and the first synchronization interface (also called synchronization port) (`synchport1`) of both FortiManager units in the cluster. The local IP1 IP address of both FortiManager units must match the peer IP1 IP address of the other FortiManager unit. Both units should also have the same first synchronization interface.

Syntax

```
config system ha
    set clusterid <clusert_ID_int>
    set file-quota <integer>
    set hb-interval <time_interval_int>
    set hb-lost-threshold <lost_heartbeats_int>
    set mode {master | slave | standalone}
    set password <password_string>
    config peer
        edit <peer_id_int>
            set ip <ipv4_address>
            set serial-number <peer_serial_str>
            set status <peer_status>
        end
    end
end
```

Variable	Description
<code>clusterid</code> <code><clusert_ID_int></code>	A number between 0 and 64 that identifies the HA cluster. All members of the HA cluster must have the same <code>clusterid</code> . If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different group ID.
<code>file-quota</code> <code><integer></code>	Set the file quota in MB (2048 to 20480).
<code>hb-interval</code> <code><time_interval_int></code>	The time in seconds that a cluster unit waits between sending heartbeat packets. The heartbeat interval is also the amount of time that a cluster unit waits before expecting to receive a heartbeat packet from the other cluster unit. The default heartbeat interval is 5 seconds. The default heartbeat interval is 5 seconds. The heartbeat interval range is 1 to 255 seconds.

Variable	Description
<pre>hb-lost- threshold <lost_ heartbeats_ int></pre>	<p>The number of heartbeat intervals that one of the cluster units waits to receive HA heartbeat packets from other cluster units before assuming that the other cluster units have failed.</p> <p>The default failover threshold is 3. The failover threshold range is 1 to 255. In most cases you do not have to change the heartbeat interval or failover threshold. The default settings mean that if the a unit fails, the failure is detected after 3 x 5 or 15 seconds; resulting in a failure detection time of 15 seconds. If the failure detection time is too short the HA cluster may detect a failure when none has occurred.</p> <p>For example, if the primary unit is very busy it may not respond to HA heartbeat packets in time. In this situation, the backup unit may assume that the primary unit has failed when the primary unit is actually just busy. Increase the failure detection time to prevent the backup unit from detecting a failure when none has occurred.</p> <p>If the failure detection time is too long, administrators will be delayed in learning that the cluster has failed. In most cases, a relatively long failure detection time will not have a major effect on operations. But if the failure detection time is too long for your network conditions, then you can reduce the heartbeat interval or failover threshold.</p>
<pre>mode {master slave standalone}</pre>	<p>Type <code>master</code> to configure the FortiManager unit to be the primary unit in a cluster. Type <code>slave</code> to configure the FortiManager unit to be a backup unit in a cluster. Type <code>standalone</code> to stop operating in HA mode.</p>
<pre>password <password_ string></pre>	<p>A group password for the HA cluster. All members of the HA cluster must have the same group password. The maximum password length is 19 characters. If you have more than one FortiManager HA cluster on the same network, each HA cluster must have a different password.</p>
<p>Variables for <code>config peer</code> subcommand:</p> <p>Add peers to the HA configuration of the FortiManager unit. You add all of the backup units as peers to the primary unit (up to four). For each backup unit you add the primary unit.</p>	
<pre><peer_id_int></pre>	<p>Add a peer and add the peer's IP address and serial number.</p>
<pre>ip <ipv4_ address></pre>	<p>Enter the IPv4 address of the peer FortiManager unit.</p>
<pre>serial-number <peer_ serial_str></pre>	<p>Enter the serial number of the peer FortiManager unit.</p>
<pre>status <peer_ status></pre>	<p>Enter the status of the peer FortiManager unit.</p>

General FortiManager HA configuration steps

The following steps assume that you are starting with four FortiManager units running the same firmware build and are set to the factory default configuration. The primary unit and the first backup unit are connected to the

same network. The second and third backup units are connected to a remote network and communicate with the primary unit over the Internet.

1. Enter the following command to configure the primary unit for HA operation.

```
config system ha
  set mode master
  set password <password_str>
  set clusterid 10
  config peer
    edit 1
      set ip <peer_ip_ipv4>
      set serial-number <peer_serial_str>
    next
    edit 2
      set ip <peer_ip_ipv4>
      set serial-number <peer_serial_str>
    next
    edit 3
      set ip <peer_ip_ipv4>
      set serial-number <peer_serial_str>
    next
  end
```

This command configures the FortiManager unit to operate as the primary unit, adds a password, sets the `clusterid` to 10, and accepts defaults for the other HA settings. This command also adds the three backup units to the primary unit as peers.

2. Enter the following command to configure the backup units for HA operation.

```
config system ha
  set mode slave
  set password <password_str>
  set clusterid 10
  config peer
    edit 1
      set ip <peer_ip_ipv4>
      set serial-number <peer_serial_str>
    next
  end
```

This command configures the FortiManager unit to operate as a backup unit, adds the same password, and `clusterid` as the primary unit, and accepts defaults for the other HA settings. This command also adds the primary unit to the backup unit as a peer.

3. Repeat step 2 to configure each backup unit.

interface

Use this command to edit the configuration of a FortiManager network interface.

Syntax

```
config system interface
  edit <port_string>
    set status {up | down}
    set ip <ipv4_mask>
    set allowaccess {http https ping snmp ssh telnet webservice}
```



```

set serviceaccess {fclupdates fgtupdates webfilter-antispam}
set speed {1000full 100full 100half 10full 10half auto}
set description <string>
set alias <string>
config <ipv6>
    set ip6-address <IPv6 prefix>
    set ip6-allowaccess {http https ping snmp ssh telnet webservice}
end
end

```

Variable	Description
<port_string>	<port_str> can be set to a port number such as port1, port2, port3, or port4. Different FortiManager models have different numbers of ports.
status {up down}	Start or stop the interface. If the interface is stopped it does not accept or send packets. If you stop a physical interface, VLAN interfaces associated with it also stop. Default: up
ip <ipv4_mask>	Enter the interface IPv4 address and netmask. The IPv4 address cannot be on the same subnet as any other interface.
allowaccess {http https ping snmp ssh telnet webservice}	Enter the types of management access permitted on this interface. Separate multiple selected types with spaces. If you want to add or remove an option from the list, retype the list as required.
serviceaccess {fclupdates fgtupdates webfilter- antispam}	Enter the types of service access permitted on this interface. Separate multiple selected types with spaces. If you want to add or remove an option from the list, retype the list as required.
speed {1000full 100full 100half 10full 10half auto}	Enter the speed and duplexing the network port uses. Enter <code>auto</code> to automatically negotiate the fastest common speed. Default: <code>auto</code>
description <string>	Enter a description of the interface.
alias <string>	Enter an alias for the interface.
<ipv6>	Configure the interface IPv6 settings.
ip6-address <IPv6 prefix>	IPv6 address/prefix of interface.
ip6-allowaccess {http https ping snmp ssh telnet webservice}	Allow management access to the interface.

Example

This example shows how to set the FortiManager port1 interface IP address and network mask to 192.168.100.159 255.255.255.0, and the management access to ping, https, and ssh.

```
config system interface
  edit port1
    set allowaccess ping https ssh
    set ip 192.168.110.26 255.255.255.0
    set status up
  end
```

locallog

Use the following commands to configure local log settings.

locallog disk setting

Use this command to configure the disk settings for uploading log files, including configuring the severity of log levels.

status must be enabled to view diskfull, max-log-file-size, and upload variables.

upload must be enabled to view/set other upload* variables.

Syntax

```
config system locallog disk setting
  set status {enable | disable}
  set severity {alert | critical | debug | emergency | error | information |
    notification | warning}
  set max-log-file-size <size_int>
  set roll-schedule {none | daily | weekly}
  set roll-day <string>
  set roll-time <hh:mm>
  set diskfull {nolog | overwrite}
  set log-disk-full-percentage <integer>
  set upload {disable | enable}
  set uploadip <ipv4_address>
  set server-type {FAZ | FTP | SCP | SFTP}
  set uploadport <port_int>
  set uploaduser <user_str>
  set uploadpass <password_string>
  set uploadaddr <dir_str>
  set uploadtype <event>
  set uploadzip {disable | enable}
  set uploadsched {disable | enable}
  set upload-time <hh:mm>
  set upload-delete-files {disable | enable}
end
```

Variable	Description
status {enable disable}	Enter <code>enable</code> to begin logging. Default: <code>disable</code>
severity {alert critical debug emergency error information notification warning}	<p>Select the logging severity level. The FortiManager unit logs all messages at and above the logging severity level you select. For example, if you select <code>critical</code>, the unit logs <code>critical</code>, <code>alert</code>, and <code>emergency</code> level messages. Default: <code>alert</code></p> <p>The logging levels in descending order are:</p> <ul style="list-style-type: none"> • <code>emergency</code>: The unit is unusable. • <code>alert</code>: Immediate action is required. • <code>critical</code>: Functionality is affected. • <code>error</code>: Functionality is probably affected. • <code>warning</code>: Functionality might be affected. • <code>notification</code>: Information about normal events. • <code>information</code>: General information about unit operations. • <code>debug</code>: Information used for diagnosis or debugging.
max-log-file-size <size_int>	Enter the size at which the log is rolled. The range is from 1 to 1024 megabytes. Default: <code>100</code>
roll-schedule {none daily weekly}	Enter the period for the scheduled rolling of a log file. If <code>roll-schedule</code> is <code>none</code> , the log rolls when <code>max-log-file-size</code> is reached. Default: <code>none</code>
roll-day <string>	Enter the day for the scheduled rolling of a log file.
roll-time <hh:mm>	Enter the time for the scheduled rolling of a log file.
diskfull {nolog overwrite}	<p>Enter action to take when the disk is full:</p> <ul style="list-style-type: none"> • <code>nolog</code>: stop logging • <code>overwrite</code>: overwrites oldest log entries <p>Default: <code>overwrite</code></p>
log-disk-full-percentage <integer>	Enter the percentage at which the log disk will be considered full (50-90%).
upload {disable enable}	Enable to permit uploading of logs. Default: <code>disable</code>
uploadip <ipv4_address>	Enter IPv4 address of the destination server. Default: <code>0.0.0.0</code>
server-type {FAZ FTP SCP SFTP}	Enter the type the server to use to store the logs.

Variable	Description
uploadport <port_ int>	Enter the port to use when communicating with the destination server. Default: 21
uploaduser <user_ str>	Enter the user account on the destination server.
uploadpass <password_ string>	Enter the password of the user account on the destination server.
uploaddir <dir_ str>	Enter the destination directory on the remote server.
uploadtype <event>	Enter to upload the event log files. Default: event
uploadzip {disable enable}	Enable to compress uploaded log files. Default: disable
uploadsched {disable enable}	Enable to schedule log uploads.
upload-time <hh:mm>	Enter to configure when to schedule an upload.
upload-delete- files {disable enable}	Enable to delete log files after uploading. Default: enable

Example

In this example, the logs are uploaded to an upload server and are not deleted after they are uploaded.

```

config system locallog disk setting
    set status enable
    set severity information
    set max-log-file-size 1000MB
    set roll-schedule daily
    set upload enable
    set uploadip 10.10.10.1
    set uploadport port 443
    set uploaduser myname2
    set uploadpass 12345
    set uploadtype event
    set uploadzip enable
    set uploadsched enable
    set upload-time 06:45
    set upload-delete-file disable
end

```

locallog filter

Use this command to configure filters for local logs. All keywords are visible only when `event` is enabled.

Syntax

```
config system locallog [memory| disk | fortianalyzer | syslogd | syslogd2 | syslogd3]
  filter
    set devcfg {disable | enable}
    set devops {enable | disable}
    set dm {disable | enable}
    set dvm {disable | enable}
    set epmgr {disable | enable}
    set event {disable | enable}
    set faz {enable | disable}
    set fgd {disable | enable}
    set fgfm {disable | enable}
    set fips {disable | enable}
    set fmgws {disable | enable}
    set fmlmgr {disable | enable}
    set fmwmgr {disable | enable}
    set glbcfg {disable | enable}
    set ha {disable | enable}
    set iolog {disable | enable}
    set logd {disable | enable}
    set lrmgr {disable | enable}
    set objcfg {disable | enable}
    set rev {disable | enable}
    set rtmon {disable | enable}
    set scfw {disable | enable}
    set scply {disable | enable}
    set scrmgr {disable | enable}
    set scvpn {disable | enable}
    set system {disable | enable}
    set webport {disable | enable}
  end
```

Variable	Description
devcfg {disable enable}	Enable to log device configuration messages.
devops {enable disable}	Enable/disable managed device operations messages.
dm {disable enable}	Enable to log deployment manager messages. Default: disable
dvm {disable enable}	Enable to log device manager messages. Default: disable
epmgr {disable enable}	Enable to log endpoint manager messages. Default: disable

Variable	Description
event {disable enable}	Enable to configure log filter messages. Default: disable
faz {enable disable}	Enable to log FortiAnalyzer messages. Default: disable
fgd {disable enable}	Enable to log FortiGuard service messages. Default: disable
fgfm {disable enable}	Enable to log FortiGate/FortiManager communication protocol messages. Default: disable
fips {disable enable}	Enable to log FIPS messages. Default: disable
fmgws {disable enable}	Enable to log web service messages. Default: disable
fmlmgr {disable enable}	Enable to log FortiMail manager messages. Default: disable
fmwmgr {disable enable}	Enable to log firmware manager messages. Default: disable
glbcfg {disable enable}	Enable to log global database messages. Default: disable
ha {disable enable}	Enable to log high availability activity messages. Default: disable
iolog {disable enable}	Enable input/output log activity messages. Default: disable
logd {disable enable}	Enable logd messages. Default: disable
lrmgr {disable enable}	Enable to log log and report manager messages. Default: disable
objcfg {disable enable}	Enable to log object configuration. Default: disable
rev {disable enable}	Enable to log revision history messages. Default: disable
rtmon {disable enable}	Enable to log real-time monitor messages. Default: disable

Variable	Description
scfw {disable enable}	Enable to log firewall objects messages. Default: disable
scply {disable enable}	Enable to log policy console messages. Default: disable
scrmgr {disable enable}	Enable to log script manager messages. Default: disable
scvpn {disable enable}	Enable to log VPN console messages. Default: disable
system {disable enable}	Enable to log system manager messages. Default: disable
webport {disable enable}	Enable to log web portal messages. Default: disable

Example

In this example, the local log filters are log and report manager, and system settings. Events in these areas of the FortiManager unit will be logged.

```
config system locallog filter
  set event enable
  set lrmgr enable
  set system enable
end
```

locallog fortianalyzer setting

Use this command to enable or disable, and select the severity threshold of, remote logging to the FortiAnalyzer unit entered in `system log fortianalyzer`.

The severity threshold required to forward a log message to the FortiAnalyzer unit is separate from event, syslog, and local logging severity thresholds.

Syntax

```
config system locallog fortianalyzer setting
  set severity {emergency | alert | critical | error | warning | notification |
  information | debug}
  set status {disable | enable}
end
```

Variable	Description
severity {emergency alert critical error warning notification information debug}	Enter the severity threshold that a log message must meet or exceed to be logged to the unit. Default: alert
status {disable enable}	Enable/disable remote logging to the FortiAnalyzer unit. Default: disable

Example

You might enable remote logging to the FortiAnalyzer unit configured. Events at the information level and higher, which is everything except debug level events, would be sent to the FortiAnalyzer unit.

```
config system locallog fortianalyzer setting
  set status enable
  set severity information
end
```

locallog memory setting

Use this command to configure memory settings for local logging purposes.

Syntax

```
config system locallog memory setting
  set diskfull {nolog | overwrite}
  set severity {emergency | alert | critical | error | warning | notification |  
information | debug}
  set status <disable | enable>
end
```

Variable	Description
diskfull {nolog overwrite}	Enter the action to take when the disk is full: <ul style="list-style-type: none"> nolog: Stop logging when disk full overwrite: Overwrites oldest log entries
severity {emergency alert critical error warning notification information debug}	Enter to configure the severity level to log files. Default: alert
status <disable enable>	Enable/disable the memory buffer log. Default: disable

Example

This example shows how to enable logging to memory for all events at the notification level and above. At this level of logging, only information and debug events will not be logged.

```
config system locallog memory
    set severity notification
    set status enable
end
```

locallog syslogd (syslogd2, syslogd3) setting

Use this command to configure the settings for logging to a syslog server. You can configure up to three syslog servers; syslogd, syslogd2 and syslogd3.

Syntax

```
config system locallog {syslogd | syslogd2 | syslogd3} setting
    set csv {disable | enable}
    set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp |
        kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 |
        lpr | mail | news | ntp | syslog | user | uucp}
    set severity {emergency | alert | critical | error | warning | notification |
        information | debug}
    set status {enable | disable}
    set syslog-name <string>
end
```

Variable	Description
csv {disable enable}	Enable to produce the log in comma separated value (CSV) format. If you do not enable CSV format the FortiManager unit produces space separated log files. Default: disable

Variable	Description
<pre> facility {alert audit auth authpriv clock cron daemon ftp kernel local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news ntp syslog user uucp} </pre>	<p>Enter the facility type. <code>facility</code> identifies the source of the log message to syslog. Change <code>facility</code> to distinguish log messages from different FortiManager units so you can determine the source of the log messages. Available facility types are:</p> <ul style="list-style-type: none"> • <code>alert</code>: log alert • <code>audit</code>: log audit • <code>auth</code>: security/authorization messages • <code>authpriv</code>: security/authorization messages (private) • <code>clock</code>: clock daemon • <code>cron</code>: cron daemon performing scheduled commands • <code>daemon</code>: system daemons running background system processes • <code>ftp</code>: File Transfer Protocol (FTP) daemon • <code>kernel</code>: kernel messages • <code>local0</code>: <code>local17</code> — reserved for local use • <code>lpr</code>: line printer subsystem • <code>mail</code>: email system • <code>news</code>: network news subsystem • <code>ntp</code>: Network Time Protocol (NTP) daemon • <code>syslog</code>: messages generated internally by the syslog daemon. <p>Default: <code>local7</code></p>
<pre> severity {emergency alert critical error warning notification information debug} </pre>	<p>Select the logging severity level. The FortiManager unit logs all messages at and above the logging severity level you select. For example, if you select <code>critical</code>, the unit logs <code>critical</code>, <code>alert</code>, and <code>emergency</code> level messages. The logging levels in descending order are:</p> <ul style="list-style-type: none"> • <code>emergency</code>: The unit is unusable. • <code>alert</code>: Immediate action is required. • <code>critical</code>: Functionality is affected. • <code>error</code>: Functionality is probably affected. • <code>warning</code>: Functionality might be affected. • <code>notification</code>: Information about normal events. • <code>information</code>: General information about unit operations. • <code>debug</code>: Information used for diagnosis or debugging.
<pre> status {enable disable} </pre>	Enter <code>enable</code> to begin logging.
<pre> syslog-name <string> </pre>	Enter the remote syslog server name.

Example

In this example, the logs are uploaded to a syslog server at IP address `10.10.10.8`. The FortiManager unit is identified as facility `local0`.

```

config system locallog syslogd setting
    set facility local0

```

```
    set status enable
    set severity information
end
```

log

Use the following commands to configure log settings.

log alert

Use this command to configure log based alert settings.

Syntax

```
config system log alert
    set max-alert-count <integer>
end
```

Variable	Description
max-alert-count <integer>	The alert count range, between 100 and 1000.

log fortianalyzer

Use this command to configure a connection with the FortiAnalyzer unit which will be used as the FortiManager's remote log server. You must configure the FortiAnalyzer unit to accept web service connections.

Syntax

```
config system log fortianalyzer
    set status {disable | enable}
    set ip <ipv4>
    set secure_connection {disable | enable}
    set localid <string>
    set psk <password_string>
    set username <username_string>
    set passwd <password_string>
    set auto_install {enable | disable}
end
```

Variable	Description
status {disable enable}	Enable/disable to configure the connection to the FortiAnalyzer unit. Default: disable
ip <ipv4>	Enter the IP address of the FortiAnalyzer unit.
secure_connection {disable enable}	Enable/disable secure connection with the FortiAnalyzer unit.

Variable	Description
localid <string>	Enter the local ID.
psk <password_string>	Enter the preshared key with the FortiAnalyzer unit.
username <username_string>	Enter the FortiAnalyzer administrator login that the FortiManager unit will use to administer the FortiAnalyzer unit.
passwd <password_string>	Enter the FortiAnalyzer administrator password for the account specified in username.
auto_install {enable disable}	Enable to automatically update the FortiAnalyzer settings as they are changed on the FortiManager unit. Default: disable

Example

You can configure a secure tunnel for logs and other communications with the FortiAnalyzer unit.

```
config system log fortianalyzer
    set status enable
    set ip 192.168.1.100
    set username admin
    set passwd wert5W34bNg
end
```

log settings

Use this command to configure settings for logs.

Syntax

```
config system log settings
    set FCH-custom-field1 <string>
    set FCT-custom-field1 <string>
    set FGT-custom-field1 <string>
    set FML-custom-field1 <string>
    set FWB-custom-field1 <string>
    set FAZ-custom-field1 <string>
    set FSA-custom-field1 <string>
    set log-file-archive-name {basic | extended}
    set sync-search-timeout <integer>
config rolling-regular
    set days {fri | mon | sat | sun | thu | tue | wed}
    set del-files {disable | enable}
    set directory <string>
    set file-size <integer>
    set gzip-format {disable | enable}
    set hour <integer>
    set ip <ipv4_address>
    set ip2 <ipv4_address>
    set ip3 <ipv4_address>
    set log-format {csv | native | text}
    set min <integer>
    set password <string>
```

```

    set password2 <string>
    set password3 <string>
    set server-type {ftp | scp | sftp}
    set upload {disable | enable}
    set upload-hour <integer>
    set upload-mode backup
    set upload-trigger {on-roll | on-schedule}
    set username <string>
    set username2 <string>
    set username3 <string>
    set when {daily | none | weekly}
end
end

```

Variable	Description
FCH-custom-field1 <string>	Enter a name of the custom log field to index.
FCT-custom-field1 <string>	Enter a name of the custom log field to index.
FGT-custom-field1 <string>	Enter a name of the custom log field to index.
FML-custom-field1 <string>	Enter a name of the custom log field to index.
FWB-custom-field1 <string>	Enter a name of the custom log field to index.
FAZ-custom-field1 <string>	Enter a name of the custom log field to index.
FSA-custom-field1 <string>	Enter a name of the custom log field to index.
log-file-archive-name {basic extended}	Log file name format for archiving, such as backup, upload or download. <ul style="list-style-type: none"> • basic: Basic format for log archive file name, e.g. FGT20C0000000001.tlog.1417797247.log. • extended: Extended format for log archive file name, e.g. FGT20C0000000001.2014-12-05-08:34:58.tlog.1417797247.log.
sync-search-timeout <integer>	The maximum number of seconds that a log search session can run in synchronous mode.

Variables for config rolling-regular **subcommand**:

Variable	Description
days {fri mon sat sun thu tue wed}	Log files rolling schedule (days of the week). When when is set to weekly, you can configure days, hour, and min values.
del-files {disable enable}	Enable/disable log file deletion after uploading.
directory <string>	The upload server directory.
file-size <integer>	Roll log files when they reach this size (MB).
gzip-format {disable enable}	Enable/disable compression of uploaded log files.
hour <integer>	Log files rolling schedule (hour).
ip <ipv4_ address> ip2 <ipv4_ address> ip3 <ipv4_ address>	Upload server IP addresses. Configure up to three servers.
log-format {csv native text}	Format of uploaded log files.
min <integer>	Log files rolling schedule (minutes).
password <string> password2 <string> password3 <string>	Upload server login passwords.
server-type {ftp scp sftp}	Upload server type.
upload {disable enable}	Enable/disable log file uploads.
upload-hour <integer>	Log files upload schedule (hour).

Variable	Description
upload-mode backup	Configure upload mode with multiple servers. Servers are attempted and used one after the other upon failure to connect.
upload-trigger {on-roll on-schedule}	Event triggering log files upload: <ul style="list-style-type: none"> on-roll: Upload log files after they are rolled. on-schedule: Upload log files daily.
username <string> username2 <string> username3 <string>	Upload server login usernames.
when {daily none weekly}	Roll log files periodically.

mail

Use this command to configure mail servers on your FortiManager unit.

Syntax

```
config system mail
  edit <server>
    set auth {enable | disable}
    set passwd <password_string>
    set port <port>
    set user <string>
  end
```

Variable	Description
<server>	Enter the name of the mail server.
auth {enable disable}	Enable/disable authentication.
passwd <password_ string>	Enter the SMTP account password value.
port <port>	Enter the SMTP server port.
user <string>	Enter the SMTP account user name.

metadata

Use this command to add additional information fields to the administrator accounts of your FortiManager unit.



This command creates the metadata fields. Use `config system admin user` to add data to the metadata fields.

Syntax

```
config system metadata admins
  edit <fieldname>
    set field_length {20 | 50 | 255}
    set importance {optional | required}
    set status {enable | disable}
  end
```

Variable	Description
<fieldname>	Enter the name of the field.
field_length {20 50 255}	Select the maximum number of characters allowed in this field: 20, 50, or 255. Default: 50
importance {optional required}	Select if this field is required or optional when entering standard information. Default: optional
status {enable disable}	Enable/disable the metadata. Default: disable

ntp

Use this command to configure automatic time setting using a network time protocol (NTP) server.

Syntax

```
config system ntp
  set status {enable | disable}
  set sync_interval <min_str>
  config ntpserver
    edit <id>
      set ntpv3 {disable | enable}
      set server {<ipv4> | <fqdn_str>}
      set authentication {disable | enable}
      set key <password_string>
      set key-id <integer>
    end
  end
```


Variable	Description
status {enable disable}	Enable/disable NTP time setting. Default: disable
sync_interval <min_str>	Enter time, in minutes, how often the FortiManager unit synchronizes its time with the NTP server. Default: 60
Variables for config ntpserver subcommand:	
ntp3 {disable enable}	Enable/disable NTPV3. Default: disable
server {<ipv4> <fqdn_str>}	Enter the IP address or fully qualified domain name of the NTP server.
authentication {disable enable}	Enable/disable MD5 authentication. Default: disable
key <password_string>	The authentication key.
key-id <integer>	The key ID for authentication. Default: 0

password-policy

Use this command to configure access password policies.

Syntax

```
config system password-policy
  set status {disable | enable}
  set minimum-length <integer>
  set must-contain <lower-case-letter | non-alphanumeric | number | upper-case-letter>
  set change-4-characters {disable | enable}
  set expire <integer>
end
```

Variable	Description
status {disable enable}	Enable/disable the password policy. Default: enable
minimum-length <integer>	Set the password's minimum length. Must contain between 8 and 256 characters. Default: 8

Variable	Description
<code>must-contain <lower-case-letter non-alphanumeric number upper-case-letter></code>	Characters that a password must contain. <ul style="list-style-type: none"> <code>lower-case-letter</code>: the password must contain at least one lower case letter <code>non-alphanumeric</code>: the password must contain at least one non-alphanumeric characters <code>number</code>: the password must contain at least one number <code>upper-case-letter</code>: the password must contain at least one upper case letter.
<code>change-4-characters {disable enable}</code>	Enable/disable changing at least 4 characters for a new password. Default: <code>disable</code>
<code>expire <integer></code>	Set the number of days after which admin users' password will expire; 0 means never. Default: 0

report

Use the following command to configure report related settings.

report auto-cache

Use this command to view or configure report auto-cache settings.

Syntax

```

config system report auto-cache
    set aggressive-drilldown {enable | disable}
    set aggressive-schedule {enable | disable}
    set drilldown-interval <integer>
    set drilldown-status {enable | disable}
    set order {latest-first | oldest-first}
    set status {enable | disable}
end

```

Variable	Description
<code>aggressive-drilldown {enable disable}</code>	Enable/disable the aggressive drill-down <code>auto-cache</code> .
<code>aggressive-schedule {enable disable}</code>	Enable/disable <code>auto-cache</code> on schedule reports aggressively.

Variable	Description
drilldown-interval <integer>	The time interval in hours for drill-down auto-cache.
drilldown-status {enable disable}	Enable/disable drill-down auto-cache.
order {latest-first oldest-first}	The order of which SQL log table is processed first. <ul style="list-style-type: none"> latest-first: The latest SQL log table is processed first. oldest-first: The oldest SQL log table is processed first.
status {enable disable}	Enable/disable the SQL report auto-cache.

report est-browse-time

Use this command to view or configure report settings.

Syntax

```
config system report est-browse-time
  set max-num-user <integer>
  set status {enable | disable}
end
```

Variable	Description
max-num-user <integer>	Set the maximum number of users to estimate browse time.
status {enable disable}	Enable/disable estimating browse time.

report group

Use these commands to configure report grouping.

Syntax

```
config system report group
  edit <group-id>
    set adom <ADOM name>
    set case-insensitive {enable | disable}
    set report-like <string>
  next
config chart-alternative
  edit <chart-name>
    set chart-replace <string>
config group-by
  edit <variable-name>
    set var-expression <string>
```

end

Variable	Description
<group-id>	Enter the report group ID or enter a new name to create a new entry.
<ADOM name>	Enter the ADOM name.
case-insensitive {enable disable}	Enable/disable case insensitive match. <ul style="list-style-type: none"> disable: Disable the case insensitive match. enable: Enable the case insensitive match.
report-like <string>	Enter the report name string.
Variables for config chart-alternative subcommand:	
<group-id>	Enter the report group ID or enter a new name to create a new entry.
<ADOM name>	Enter the ADOM name.
case-insensitive {enable disable}	Enable/disable case insensitive match. <ul style="list-style-type: none"> disable: Disable the case insensitive match. enable: Enable the case insensitive match.
report-like <string>	Enter the report name string.
Variables for config group-by subcommand:	
<var-name>	Enter the variable name or enter a new name to create a new entry.
var-expression <string>	Enter the variable expression.

report setting

Use these commands to view or configure report settings.

Syntax

```
config system report setting
  set hcache-lossless {enable | disable}
  set max-table-rows <integer>
  set report-priority {low | normal}
  set week-start {mon | sun}
end
```

Variable	Description
hcache-lossless {enable disable}	Enable/disable hcache lossless. <ul style="list-style-type: none"> disable: Use ready-with-loss hcache. enable: Do not use ready-with-loss hcache.
max-table-rows <integer>	Set the maximum number of rows that can be generated in a single table. Range: 10000 to 100000
report-priority {low normal}	Priority of SQL report. <ul style="list-style-type: none"> low: Low normal: Normal
week-start {mon sun}	Set the day that the week starts on, either Sunday or Monday.

Use the `show` command to display the current configuration if it has been changed from its default value:

```
show system report settings
```

route

Use this command to view or configure static routing table entries on your FortiManager unit.

Syntax

```
config system route
edit <seq_int>
set device <port_str>
set dst <dst_ipv4mask>
set gateway <ipv4_address>
end
```

Variable	Description
<seq_int>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.
device <port_str>	Enter the port used for this route.
dst <dst_ipv4mask>	Enter the IP address and mask for the destination network.
gateway <ipv4_address>	Enter the default gateway IP address for this network.

route6

Use this command to view or configure static IPv6 routing table entries on your FortiManager unit.

Syntax

```
config system route6
  edit <seq_int>
    set device <string>
    set dst <ipv6_address>
    set gateway <ipv6_address>
  end
```

Variable	Description
<seq_int>	Enter an unused routing sequence number to create a new route. Enter an existing route number to edit that route.
device <string>	Enter the port used for this route.
dst <ipv6_address>	Enter the IP address and mask for the destination network.
gateway <ipv6_address>	Enter the default gateway IP address for this network.

snmp

Use the following commands to configure SNMP related settings.

snmp community

Use this command to configure SNMP communities on your FortiManager unit.

You add SNMP communities so that SNMP managers, typically applications running on computers to monitor SNMP status information, can connect to the FortiManager unit (the SNMP agent) to view system information and receive SNMP traps. SNMP traps are triggered when system events happen such as when there is a system restart, or when the log disk is almost full.

You can add up to three SNMP communities, and each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiManager unit for a different set of events.

Hosts are the SNMP managers that make up this SNMP community. Host information includes the IP address and interface that connects it to the FortiManager unit.

For more information on SNMP traps and variables, see the [Fortinet Document Library](#).



Part of configuring an SNMP manager is to list it as a host in a community on the FortiManager unit that it will be monitoring. Otherwise that SNMP manager will not receive any traps or events from the FortiManager unit, and will be unable to query the FortiManager unit as well.

Syntax

```
config system snmp community
  edit <index_number>
```

```

set events <events_list>
set name <community_name>
set query-v1-port <port_number>
set query-v1-status {enable | disable}
set query-v2c-port <port_number>
set query-v2c-status {enable | disable}
set status {enable | disable}
set trap-v1-rport <port_number>
set trap-v1-status {enable | disable}
set trap-v2c-rport <port_number>
set trap-v2c-status {enable | disable}
config hosts
    edit <host_number>
        set interface <if_name>
        set ip <ipv4_address>
    end
end

```

Variable	Description
<index_number>	Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community.
events <events_list>	<p>Enable the events for which the FortiManager unit should send traps to the SNMP managers in this community. The <code>raid_changed</code> event is only available for devices which support RAID.</p> <ul style="list-style-type: none"> • <code>cpu-high-exclude-nice</code>: CPU usage exclude NICE threshold. • <code>cpu_high</code>: CPU usage too high. • <code>disk_low</code>: Disk usage too high. • <code>ha_switch</code>: HA switch. • <code>intf_ip_chg</code>: Interface IP address changed. • <code>lic-dev-quota</code>: High licensed device quota detected. • <code>lic-gbday</code>: High licensed log GB/day detected. • <code>log-alert</code>: Log base alert message. • <code>log-data-rate</code>: High incoming log data rate detected. • <code>log-rate</code>: High incoming log rate detected. • <code>mem_low</code>: Available memory is low. • <code>raid_changed</code>: RAID status changed. • <code>sys_reboot</code>: System reboot. <p>Default: All events enabled</p>
name <community_name>	<p>Enter the name of the SNMP community. Names can be used to distinguish between the roles of the hosts in the groups. For example the Logging and Reporting group would be interested in the <code>disk_low</code> events, but likely not the other events. The name is included in SNMPv2c trap packets to the SNMP manager, and is also present in query packets from, the SNMP manager.</p>

Variable	Description
query-v1-port <port_number>	Enter the SNMPv1 query port number used when SNMP managers query the FortiManager unit. Default: 161
query-v1-status {enable disable}	Enable/disable SNMPv1 queries for this SNMP community. Default: enable
query-v2c-port <port_number>	Enter the SNMPv2c query port number used when SNMP managers query the FortiManager unit. SNMP v2c queries will include the name of the community. Default: 161
query-v2c-status {enable disable}	Enable/disable SNMPv2c queries for this SNMP community. Default: enable
status {enable disable}	Enable/disable this SNMP community. Default: enable
trap-v1-rport <port_number>	Enter the SNMPv1 remote port number used for sending traps to the SNMP managers. Default: 162
trap-v1-status {enable disable}	Enable/disable SNMPv1 traps for this SNMP community. Default: enable
trap-v2c-rport <port_number>	Enter the SNMPv2c remote port number used for sending traps to the SNMP managers. Default: 162
trap-v2c-status {enable disable}	Enable/disable SNMPv2c traps for this SNMP community. SNMPv2c traps sent out to SNMP managers include the community name. Default: enable
Variables for config hosts subcommand:	
<host_number>	Enter the index number of the host in the table. Enter an unused index number to create a new host.
interface <if_name>	Enter the name of the FortiManager unit that connects to the SNMP manager.
ip <ipv4_address>	Enter the IPv4 address of the SNMP manager. Default: 0.0.0.0

Example

This example shows how to add a new SNMP community named SNMP_Com1. The default configuration can be used in most cases with only a few modifications. In the example below the community is added, given a name, and then because this community is for an SNMP manager that is SNMPv1 compatible, all v2c functionality is disabled. After the community is configured the SNMP manager, or host, is added. The SNMP manager IP address is 192.168.20.34 and it connects to the FortiManager unit internal interface.

```
config system snmp community
  edit 1
    set name SNMP_Com1
```



```
set query-v2c-status disable
set trap-v2c-status disable
config hosts
  edit 1
  set interface internal
  set ip 192.168.10.34
end
end
```

snmp sysinfo

Use this command to enable the FortiManager SNMP agent and to enter basic system information used by the SNMP agent. Enter information about the FortiManager unit to identify it. When your SNMP manager receives traps from the FortiManager unit, you will know which unit sent the information. Some SNMP traps indicate high CPU usage, log full, or low memory.

For more information on SNMP traps and variables, see the [Fortinet Document Library](#).

Syntax

```
config system snmp sysinfo
  set contact-info <info_str>
  set description <description>
  set engine-id <string>
  set location <location>
  set status {enable | disable}
  set trap-high-cpu-threshold <percentage>
  set trap-low-memory-threshold <percentage>
  set trap-cpu-high-exclude-nice-threshold <percentage>
end
```

Variable	Description
contact-info <info_str>	Add the contact information for the person responsible for this FortiManager unit. The contact information can be up to 35 characters long.
description <description>	Add a name or description of the FortiManager unit. The description can be up to 35 characters long.
engine-id <string>	Local SNMP engine ID string (maximum 24 characters).
location <location>	Describe the physical location of the FortiManager unit. The system location description can be up to 35 characters long.
status {enable disable}	Enable/disable the FortiManager SNMP agent. Default: disable
trap-high-cpu-threshold <percentage>	CPU usage when trap is set. Default: 80

Variable	Description
trap-low-memory-threshold <percentage>	Memory usage when trap is set. Default: 80
trap-cpu-high-exclude-nice-threshold <percentage>	CPU high usage excludes nice when the trap is sent.

Example

This example shows how to enable the FortiManager SNMP agent and add basic SNMP information.

```
config system snmp sysinfo
  set status enable
  set contact-info 'System Admin ext 245'
  set description 'Internal network unit'
  set location 'Server Room A121'
end
```

snmp user

Use this command to configure SNMPv3 users on your FortiManager unit. To use SNMPv3, you will first need to enable the FortiManager SNMP agent. For more information, see `snmp sysinfo`. There should be a corresponding configuration on the SNMP server in order to query to or receive traps from FortiManager.

For more information on SNMP traps and variables, see the [Fortinet Document Library](#).

Syntax

```
config system snmp user
  edit <name>
    set auth-proto {md5 | sha}
    set auth-pwd <password_string>
    set events <events_list>
    set notify-hosts <ipv4_address>
    set priv-proto {aes | des}
    set priv-pwd <password_string>
    set queries {enable | disable}
    set query-port <port_number>
    set security-level <level>
  end
end
```

Variable	Description
<name>	Enter a SNMPv3 user name to add, edit, or delete.
auth-proto {md5 sha}	Authentication protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable. Select one of the following: <ul style="list-style-type: none"> md5: HMAC-MD5-96 authentication protocol sha: HMAC-SHA-96 authentication protocol

Variable	Description
auth-pwd <password_ string>	Password for the authentication protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable.
events <events_ list>	<p>Enable the events for which the FortiManager unit should send traps to the SNMPv3 managers in this community. The <code>raid_changed</code> event is only available for devices which support RAID.</p> <ul style="list-style-type: none"> <code>cpu-high-exclude-nice</code>: CPU usage exclude nice threshold. <code>cpu_high</code>: The CPU usage is too high. <code>disk_low</code>: The log disk is getting close to being full. <code>ha_switch</code>: A new unit has become the HA master. <code>intf_ip_chg</code>: An interface IP address has changed. <code>lic-dev-quota</code>: High licensed device quota detected. <code>lic-gbday</code>: High licensed log GB/Day detected. <code>log-alert</code>: Log base alert message. <code>log-data-rate</code>: High incoming log data rate detected. <code>log-rate</code>: High incoming log rate detected. <code>mem_low</code>: The available memory is low. <code>raid_changed</code>: RAID status changed. <code>sys_reboot</code>: The FortiManager unit has rebooted. <p>Default: All events enabled.</p>
notify-hosts <ipv4_ address>	Hosts to send notifications (traps) to.
priv-priv {aes des}	<p>Privacy (encryption) protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable. Select one of the following:</p> <ul style="list-style-type: none"> <code>aes</code>: CFB128-AES-128 symmetric encryption protocol <code>des</code>: CBC-DES symmetric encryption protocol
priv-pwd <password_ string>	Password for the privacy (encryption) protocol. The security level must be set to <code>auth-no-priv</code> or <code>auth-priv</code> to use this variable.
queries {enable disable}	Enable/disable queries for this user. Default: <code>enable</code>
query-port <port_ number>	SNMPv3 query port Default: 161

Variable	Description
security-level <level>	<p>Security level for message authentication and encryption.</p> <ul style="list-style-type: none"> auth-no-priv: Message with authentication but no privacy (encryption). auth-priv: Message with authentication and privacy (encryption). no-auth-no-priv: Message with no authentication and no privacy (encryption). <p>Default: no-auth-no-priv</p>

sql

Configure Structured Query Language (SQL) settings.

Syntax

```

config system sql
    set database-name <string>
    set database-type <postgres>
    set device-count-high {disable | enable}
    set event-table-partition-time <integer>
    set logtype {none | app-ctrl | attack | content | dlp | emailfilter | event |
        generic | history | traffic | virus | voip | webfilter | netscan}
    set password <password_string>
    set prompt-sql-upgrade {enable | disable}
    set rebuild-event {enable | disable}
    set rebuild-event-start-time <hh:mm> <yyyy/mm/dd>
    set resend-device < >
    set reset {enable | disable}
    set server <string>
    set start-time <hh>:<mm> <yyyy>/<mm>/<dd>
    set status {disable | local | remote}
    set text-search-index {disable | enable}
    set traffic-table-partition-time <integer>
    set username <string>
    set utm-table-partition-time <integer>
    config custom-index
        edit <id>
            set device-type {FortiCache | FortiGate | FortiMail | FortiSandbox | FortiWeb}
            set index-field <Field-Name>
            set log-type <Log-Type>
        end
    config ts-index-field
        edit <category>
            set <value> <string>
        end
    end
end

```

Variable	Description
database-name <string>	Database name. Command only available when <code>status</code> is set to <code>remote</code> .
database-type <postgres>	Database type. Command only available when <code>status</code> is set to <code>local</code> or <code>remote</code> .
device-count-high	Must set to enable if the count of registered devices is greater than 8000. <ul style="list-style-type: none"> <code>disable</code>: Set to disable if device count is less than 8000. <code>enable</code>: Set to enable if device count is equal to or greater than 8000.
event-table-partition-time <integer>	Maximum SQL database table partitioning time range in minute (0 for unlimited) for event logs. SQL database table partitioning time range between 0 and 525600 minutes.
logtype {none app-ctrl attack content dlp emailfilter event generic history traffic virus voip webfilter netscan}	Log type. Command only available when <code>status</code> is set to <code>local</code> or <code>remote</code> .
password <password_string>	The password that the Fortinet unit will use to authenticate with the remote database. Command only available when <code>status</code> is set to <code>remote</code> .
prompt-sql-upgrade {enable disable}	Enable/disable prompt to convert log database into SQL database at start time in GUI.
rebuild-event {enable disable}	Enable/disable a rebuild event during SQL database rebuilding.
rebuild-event-start-time <hh:mm> <yyyy/mm/dd>	The rebuild event starting date and time.
reset {enable disable}	This command is hidden.
server <string>	Set the database ip or hostname.
start-time <hh>:<mm> <yyyy>/<mm>/<dd>	Start date and time <hh:mm yyyy/mm/dd>. Command only available when <code>status</code> is set to <code>local</code> or <code>remote</code> .

Variable	Description
status {disable local remote}	SQL database status.
text-search-index {disable enable}	Disable or enable the text search index.
traffic-table-partition-time <integer>	Maximum SQL database table partitioning time range in minute (0 for unlimited) for traffic logs. SQL database table partitioning time range between 0 and 525600 minutes.
username <string>	User name for login remote database.
utm-table-partition-time <integer>	Maximum SQL database table partitioning time range in minute (0 for unlimited) for UTM logs. SQL database table partitioning time range between 0 and 525600 minutes.

Variables for `config custom-index` subcommand:

device-type {FortiCache FortiGate FortiMail FortiSandbox FortiWeb}	Set the device type. Select one of : <ul style="list-style-type: none"> • FortiCache • FortiGate • FortiMail • FortiSandbox • FortiWeb
index-field <Field-Name>	Type a valid field name. Select one of the available field names. The available options for <code>index-field</code> is dependent on the <code>device-type</code> entry.
log-type <Log-Type>	Type the log type. The available options for <code>log-type</code> is dependent on the <code>device-type</code> entry. Select one of the available log types. <ul style="list-style-type: none"> • FortiCache: N/A • FortiGate: app-ctrl, content, dlp, emailfilter, event, netscan, traffic, virus, voip, webfilter • FortiMail: emailfilter, event, history, virus • FortiSandbox: N/A • FortiWeb: attack, event, traffic

Variables for `config ts-index-field` subcommand:

Variable	Description
<category>	<p>Category of the text search index fields. The following is the list of categories and their default fields. Select one of the following:</p> <ul style="list-style-type: none"> FGT-app-ctrl: user, group, srcip, dstip, dstport, service, app, action, status, hostname FGT-attack: severity, srcip, proto, user, attackname FGT-content: from, to, subject, action, srcip, dstip, hostname, status FGT-dlp: user, srcip, service, action, file FGT-emailfilter: user, srcip, from, to, subject FGT-event: subtype, ui, action, msg FGT-traffic: user, srcip, dstip, Service, app, utmaction, utmevent FGT-virus: service, srcip, file, virus, user FGT-voip: action, user, src, dst, from, to FGT-webfilter: user, srcip, status, catdesc FGT-netscan: user, dstip, vuln, severity, os FML-emailfilter: client_name, dst_ip, from, to, subject FML-event: subtype, msg FML-history: classifier, disposition, from, to, client_name, direction, domain, virus FML-virus: src, msg, from, to FWB-attack: http_host, http_url, src, dst, msg, action FWB-event: ui, action, msg FWB-traffic: src, dst, service, http_method, msg
<value>	Fields of the text search filter.
<string>	Select one or more field names separated with a comma. The available field names is dependent on the category selected.

syslog

Use this command to configure syslog servers.

Syntax

```

config system syslog
  edit <name>
    set ip <string>
    set port <integer>
  end

```

end

Variable	Description
ip <string>	Syslog server IP address or hostname.
port <integer>	Syslog server port.

fmupdate

Use `fmupdate` to configure settings related to FortiGuard service updates and the FortiManager unit's built-in FDS.



CLI commands and variables are case sensitive.

analyzer virusreport

Use this command to enable or disable notification of virus detection to FortiGuard.

Syntax

```
config fmupdate analyzer virusreport
  set status {enable | disable}
end
```

Variable	Description
<code>status {enable disable}</code>	Enable/disable sending virus detection notification to FortiGuard. Default: enable

Example

This example enables virus detection notifications to FortiGuard.

```
config fmupdate analyzer virusreport
  set status enable
end
```

av-ips

Use the following commands to configure antivirus and IPS related settings.

av-ips advanced-log

Use this command to enable logging of FortiGuard antivirus and IPS update packages received by the FortiManager unit's built-in FDS from the external FDS.

Syntax

```
config fmupdate av-ips advanced-log
  set log-fortigate {enable | disable}
  set log-server {enable | disable}
end
```

Variable	Description
log-fortigate {enable disable}	Enable/disable logging of FortiGuard antivirus and IPS service updates of FortiGate devices. Default: disable
log-server {enable disable}	Enable/disable logging of update packages received by the built-in FDS server. Default: disable

Example

You could enable logging of FortiGuard antivirus updates to FortiClient installations and update packages downloaded by the built-in FDS from the FDS.

```
config fmupdate av-ips advanced-log
    set log-forticlient enable
    set log-server enable
end
```

av-ips fct server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard antivirus updates for FortiClient from the FDS.

Syntax

```
config fmupdate av-ips fct server-override
    set status {enable | disable}
    config servlist
        edit <id>
            set ip <ipv4_address>
            set port <integer>
        end
    end
end
```

Variable	Description
status {enable disable}	Enable/disable the override. Default: disable
Variables for config servlist subcommand:	
<id>	Override server ID (1-10).
ip <ipv4_address>	Enter the IPv4 address of the override server address. Default: 0.0.0.0
port <integer>	Enter the Sort number to use when contacting the FDS. Default: 443

Example

You could configure the FortiManager unit's built-in FDS to use a specific FDS server and a different port when retrieving FortiGuard antivirus updates for FortiClient from the FDS.

```
config fmupdate av-ips fct server-override
```

```

set status enable
config servlist
  edit 1
    set ip 192.168.25.152
    set port 80
  end
end

```

av-ips fgt server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard antivirus and IPS updates for FortiGate units from the FDS.

Syntax

```

config fmupdate av-ips fgt server-override
  set status {enable | disable}
  config servlist
    edit <id>
      set ip <ipv4_address>
      set port <integer>
    end
  end
end

```

Variable	Description
status {enable disable}	Enable/disable the override. Default: disable
Variables for config servlist subcommand:	
<id>	Override server ID (1-10).
ip <ipv4_address>	Enter the IPv4 address of the override server address. Default: 0.0.0.0
port <integer>	Enter the Sort number to use when contacting the FDS. Default: 443

Example

You could configure the FortiManager unit's built-in FDS to use a specific FDS server and a different port when retrieving FortiGuard antivirus and IPS updates for FortiGate units from the FDS.

```

config fmupdate av-ips fgt server-override
  set status enable
  config servlist
    edit 1
      set ip 172.27.152.144
      set port 8890
    end
  end
end

```

av-ips push-override

Use this command to enable or disable push updates, and to override the default IP address and port to which the FDS sends FortiGuard antivirus and IPS push messages.

This is useful if push notifications must be sent to an IP address and/or port other than the FortiManager unit, such as the external or virtual IP address of a NAT device that forwards traffic to the FortiManager unit.

Syntax

```
config fmupdate av-ips push-override
  set ip <ipv4_address>
  set port <recipientport_int>
  set status {enable | disable}
end
```

Variable	Description
ip <ipv4_address>	Enter the external or virtual IP address of the NAT device that will forward push messages to the FortiManager unit. Default: 0.0.0.0
port <recipientport_int>	Enter the receiving port number on the NAT device. Default: 9443
status {enable disable}	Enable/disable the push updates. Default: disable

Example

You could enable the FortiManager unit's built-in FDS to receive push messages.

If there is a NAT device or firewall between the FortiManager unit and the FDS, you could also notify the FDS to send push messages to the external IP address of the NAT device, instead of the FortiManager unit's private network IP address.

```
config fmupdate av-ips push-override
  set status enable
  set ip 172.16.124.135
  set port 9000
end
```

You would then configure port forwarding on the NAT device, forwarding push messages received on User Datagram Protocol (UDP) port 9000 to the FortiManager unit on UDP port 9443.

av-ips push-override-to-client

Use this command to enable or disable push updates, and to override the default IP address and port to which the FDS sends FortiGuard antivirus and IPS push messages.

This command is useful if push notifications must be sent to an IP address and/or port other than the FortiManager unit, such as the external or virtual IP address of a NAT device that forwards traffic to the FortiManager unit.

Syntax

```
config fmupdate av-ips push-override-to-client
  set status {enable | disable}
  config <announce-ip>
    edit <id>
      set ip <ipv4_address>
      set port <recipientport_int>
```

```
end
end
```

Variable	Description
status {enable disable}	Enable/disable push updates. Default: disable
<announce-ip>	Config the IP information of the device.
<id>	Edit the announce IP ID number.
ip <ipv4_address>	Enter the announce IPv4 address. Default: 0.0.0.0
port <recipientport_int>	Enter the announce IP port. Default: 9443

av-ips update-schedule

Use this command to configure the built-in FDS to retrieve FortiGuard antivirus and IPS updates at a specified day and time.

Syntax

```
config fmupdate av-ips update-schedule
  set day {Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday}
  set frequency {every | daily | weekly}
  set status {enable | disable}
  set time <hh:mm>
end
```

Variable	Description
day {Sunday Monday Tuesday Wednesday Thursday Friday Saturday}	Enter the day of the week when the update will begin. This option only appears when the frequency is weekly.
frequency {every daily weekly}	Enter to configure the frequency of the updates. Default: every
status {enable disable}	Enable/disable regularly scheduled updates. Default: enable
time <hh:mm>	Enter to configure the time or interval when the update will begin. For example, if you want to schedule an update every day at 6:00 PM, enter 18:00. The time period format is the 24-hour clock: hh=0-23, mm=0-59. If the minute is 60, the updates will begin at a random minute within the hour. If the frequency is every, the time is interpreted as an hour and minute interval, rather than a time of day. Default: 01:60

Example

You could schedule the built-in FDS to request the latest FortiGuard antivirus and IPS updates every five hours, at a random minute within the hour.

```
config fmupdate av-ips update-schedule
  set status enable
  set frequency every
  set time 05:60
end
```

av-ips web-proxy

Use this command to configure a web proxy if FortiGuard antivirus and IPS updates must be retrieved through a web proxy.

Syntax

```
config fmupdate av-ips web-proxy
  set ip <proxy_ipv4>
  set mode {proxy | tunnel}
  set password <password_string>
  set port <port_int>
  set status {enable | disable}
  set username <username_string>
end
```

Variable	Description
ip <proxy_ipv4>	Enter the IP address of the web proxy. Default: 0.0.0.0
mode {proxy tunnel}	Enter the web proxy mode.
password <password_string>	If the web proxy requires authentication, enter the password for the user name.
port <port_int>	Enter the port number of the web proxy. Default: 80
status {enable disable}	Enable/disable connections through the web proxy. Default: disable
username <username_string>	If the web proxy requires authentication, enter the user name.

Example

You could enable a connection through a non-transparent web proxy on an alternate port.

```
config fmupdate av-ips web-proxy
  set status enable
  set mode proxy
  set ip 10.10.30.1
  set port 8890
  set username avipsupdater
  set password cvhk3rf3u9jvsYU
end
```

custom-url-list

Use this command to configure the URL database for rating and filtering. You can select to use the FortiGuard URL database, a custom URL database, or both. When selecting to use a custom URL database, use the `fmupdate {ftp | scp | tftp} import` command to import the custom URL list. When FortiManager performs the URL rating, it will check the custom URL first. If a match is found, the custom rating is returned. If there is no match, then FortiManager will check the FortiGuard database.

Syntax

```
config fmupdate custom-url-list
    set db_selection {both | custom-url | fortiguard-db}
end
```

Variable	Description
<code>db_selection</code> {both custom-url fortiguard- db}	Manage the FortiGuard URL database. <ul style="list-style-type: none">• <code>both</code>: Support both custom URL database and the FortiGuard database• <code>custom-url</code>: Customer imported URL list• <code>fortiguard-db</code>: FortiGuard database Default setting: both

device-version

Use this command to configure the correct firmware version of the device or devices connected or will be connecting to the FortiManager unit. You should verify what firmware version is currently running on the device before using this command.

Syntax

```
config fmupdate device-version
    set faz <firmware_version>
    set fct <firmware_version>
    set fgt <firmware_version>
    set fml <firmware_version>
    set fsa <firmware_version>
    set fsw <firmware_version>
end
```

Variable	Description
<code>faz <firmware_version></code>	Enter the correct firmware version that is currently running on FortiAnalyzer units. Select one of the following: <ul style="list-style-type: none">• <code>3.0</code>: Support version 3.0• <code>4.0</code>: Support version 4.0• <code>5.0</code>: Support version 5.0• <code>6.0</code>: Support version greater than 5.0

Variable	Description
fct <firmware_ version>	Enter the firmware version that is currently running for FortiClient agents. Select one of the following: <ul style="list-style-type: none"> 3.0: Support version 3.0 4.0: Support version 4.0 5.0: Support version 5.0 6.0: Support version greater than 5.0
fgt <firmware_ version>	Enter the firmware version that is currently running for FortiGate units. Select one of the following: <ul style="list-style-type: none"> 3.0: Support version 3.0 4.0: Support version 4.0 5.0: Support version 5.0 6.0: Support version greater than 5.0
fml <firmware_ version>	Enter the firmware version that is currently running for FortiMail units. Select one of the following: <ul style="list-style-type: none"> 3.0: Support version 3.0 4.0: Support version 4.0 5.0: Support version 5.0 6.0: Support version greater than 5.0
fsa <firmware_ version>	Enter the firmware version that is currently running on FortiSandbox units. Select one of the following: <ul style="list-style-type: none"> 1.0: Support version 1.0. (FortiSandbox) 2.0: Support version greater than 1.0.
fsw <firmware_ version>	Enter the firmware version that is currently running on FortiSwitch units. Select one of the following: <ul style="list-style-type: none"> 3.0: Support version 3.0 4.0: Support version 4.0 5.0: Support version 5.0 6.0: Support version greater than 5.0

Example

In the following example, the FortiGate units, including FortiClient agents, are configured with the firmware version 5.0.

```
config fmupdate device-version
  set faz 4.0
  set fct 5.0
  set fgt 5.0
end
```


disk-quota

Use this command to configure the disk space available for use by the Upgrade Manager.

If the Upgrade Manager disk space is full or if there is insufficient space to save an update package to disk, the package will not download and an alert will be sent to notify you.

Syntax

```
config fmupdate disk-quota
    set value <size_int>
end
```

Use `value` to set the size of the Upgrade Manager disk quota in megabytes (MB). The default size is 10 gigabytes (GB). If you set the disk-quota smaller than the size of an update package, the update package will not download and you will get a disk full alert.

fct-services

Use this command to configure the built-in FDS to provide FortiGuard services to FortiClient installations.

Syntax

```
config fmupdate fct-services
    set status {enable | disable}
    set port <port_int>
end
```

Variable	Description
<code>status {enable disable}</code>	Enable/disable built-in FDS service to FortiClient installations. Default: enable
<code>port <port_int></code>	Enter the port number on which the built-in FDS should provide updates to FortiClient installations. Default: 80

Example

You could configure the built-in FDS to accommodate older versions of FortiClient installations by providing service on their required port.

```
config fmupdate fct-services
    set status enable
    set port 80
end
```

fds-setting

Use this command to set FDS settings.

Syntax

```
config fmupdate fds-settings
  set fds-pull-interval <integer>
  set max-av-ips-version <integer>
end
```

Variable	Description
fds-pull-interval <integer>	Time interval FortiManager may pull updates from FDS (1 - 120 minutes).
max-av-ips-version <integer>	The maximum number of AV/IPS full version downloadable packages (1-1000).

multilayer

Use this command to set multilayer mode configuration.

Syntax

```
config fmupdate multilayer
  set webspam-rating {disable | enable}
end
```

Variable	Description
webspam-rating {disable enable}	Enable/disable URL/antispam rating service. Default: enable

publicnetwork

Use this command to enable access to the public FDS. If this function is disabled, the service packages, updates, and license upgrades must be imported manually.

Syntax

```
config fmupdate publicnetwork
  set status {disable | enable}
end
```

Variable	Description
status {disable enable}	Enable/disable the public network. Default: enable

Example

The following example shows how to enable public network.

```
config fmupdate publicnetwork
  (publicnetwork) # set status enable
end
```

server-access-priorities

Use this command to configure how a FortiGate unit may download antivirus updates and request web filtering services from multiple FortiManager units and private FDS servers.



By default, the FortiGate unit receives updates from the FortiManager unit if the FortiGate unit is managed by the FortiManager unit and the FortiGate unit was configured to receive updates from the FortiManager unit.

Syntax

```
config fmupdate server-access-priorities
  set access-public {disable | enable}
  set av-ips {disable | enable}
  set web-spam {disable | enable}
end
```

Variable	Description
access-public {disable enable}	Disable to prevent FortiManager default connectivity to public FDS and FortiGuard servers. Default: <i>enable</i>
av-ips {disable enable}	Enable to allow the FortiGate unit to get antivirus updates from other FortiManager units or private FDS servers. Default: <i>disable</i>
web-spam {disable enable}	Enable/disable private server in web-spam.

config private-server

Use this command to configure multiple FortiManager units and private servers.

Syntax

```
config fmupdate server-access-priorities
  config private-server
    edit <id>
      set ip <ipv4_address>
      set time_zone <integer>
    end
  end
end
```

Variable	Description
<id>	Enter a number to identify the FortiManager unit or private server (1 to 10).
ip <ipv4_ address>	Enter the IPv4 address of the FortiManager unit or private server.
time_zone <integer>	Enter the correct time zone of the private server. Using -24 indicates that the server is using the local time zone.

Example

The following example configures access to public FDS servers and allows FortiGate units to receive antivirus updates from other FortiManager units and private FDS servers. This example also configures three private servers.

```
config fmupdate server-access-priorities
  set access-public enable
  set av-ips enable
  config private-server
    edit 1
      set ip 172.16.130.252
    next
    edit 2
      set ip 172.31.145.201
    next
    edit 3
      set ip 172.27.122.99
    end
  end
end
```

server-override-status

Syntax

```
config fmupdate server-override-status
  set mode {loose | strict}
end
```

Variable	Description
mode {loose strict}	Set the server override mode. <ul style="list-style-type: none">• loose: allow access other servers• strict: access override server only. Default: loose

service

Use this command to enable or disable the services provided by the built-in FDS.

Syntax

```
config fmupdate service
  set avips {enable | disable}
  set query-antispam {disable | enable}
  set query-antivirus {disable | enable}
  set query-filequery {disable | enable}
  set query-webfilter {disable | enable}
  set use-cert {BIOS | FortiGuard}
end
```

Variable	Description
avips {enable disable}	Enable the built-in FDS to provide FortiGuard antivirus and IPS updates. Default: disable
query-antispam {disable enable}	Enable/disable antispam service.
query-antivirus {disable enable}	Enable/disable antivirus service.
query-filequery {disable enable}	Enable/disable file query service.
query-webfilter {disable enable}	Enable/disable web filter service.
use-cert {BIOS FortiGuard}	Choose local certificate. <ul style="list-style-type: none"> BIOS: Use default certificate in BIOS. FortiGuard: Use default certificate as FortiGuard. Default: BIOS

Example

```
config fmupdate service
  set avips enable
end
```

support-pre-fgt43

Use this command to support FortiMail 4.2 devices for FortiGuard Center updates.

Syntax

```
config fmupdate support-pre-fgt43
  set status {enable | disable}
end
```

Variable	Description
status {enable disable}	Enable/disable update support. Default: disable

web-spam

Use the following commands to configure FortiGuard antispam related settings.

web-spam fct server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard antispam updates for FortiClient from the FDS.

Syntax

```
config fmupdate web-spam fct server-override
  set status {enable | disable}
  config servlist
    edit <id>
      set ip <ipv4_address>
      set port <port_int>
    end
  end
```

Variable	Description
status {enable disable}	Enable/disable the override. Default: disable
Variables for config servlist subcommand:	
<id>	Override server ID (1-10).
ip <ipv4_address>	Enter the IPv4 address of the override server address. Default: 0.0.0.0
port <port_int>	Enter the port number to use when contacting the FDS. Default: 443

web-spam fgd-log

Use this command to configure the FortiGuard web-spam log settings.

Syntax

```
config fmupdate web-spam fgd-log
  set spamlog {all | disable | nospam}
  set status {disable | enable}
  set urllog {all | disable | miss}
end
```

Variable	Description
spamlog {all disable nospam}	Configure the anti spam log settings. <ul style="list-style-type: none"> all: Log all Spam lookups disable: Disable Spam log nospam: Log Non-spam events.
status {disable enable}	Enable/disable the FortiGuard server event log status.
urllog {all disable miss}	Configure the web filter log setting. <ul style="list-style-type: none"> all: Log all URL lookups disable: Disable URL log miss: Log URL rating misses.

web-spam fgd-setting

Use this command to configure FortiGuard run parameters.

Syntax

```

config fmupdate web-spam fgd-setting
    set as-cache <integer>
    set as-log {all | disable | nospam}
    set as-preload {disable | enable}
    set av-cache <integer>
    set av-log {all | disable | novirus}
    set av-preload {disable | enable}
    set eventlog-query {disable | enable}
    set fq-cache <integer>
    set fq-log {all | disable | nofilequery}
    set fq-preload {disable | enable}
    set linkd-log {disable | enable}
    set max-log-quota <integer>
    set max-unrated-size <integer>
    set restrict-as1-dbver <string>
    set restrict-as2-dbver <string>
    set restrict-as4-dbver <string>
    set restrict-av-dbver <string>
    set restrict-fq-dbver <string>
    set restrict-wf-dbver <string>
    set stat-log-interval <integer>
    set stat-sync-interval <integer>
    set update-interval <integer>
    set update-log {disable | enable}
    set wf-cache <integer>
    set wf-log {all | disable | nourel}
    set wf-preload {disable | enable}
end

```

Variable	Description
<code>as-cache <integer></code>	Set the antispam service maximum memory usage (100 to 2800MB).
<code>as-log {all disable nospam}</code>	Antispam log setting. Select one of the following: <ul style="list-style-type: none"> <code>all</code>: Log all spam lookups. <code>disable</code>: Disable spam log. <code>nospam</code>: Log non-spam events.
<code>as-preload {disable enable}</code>	Enable/disable preloading the antispam database into memory.
<code>av-cache <integer></code>	Set the web filter service maximum memory usage (100 to 500MB).
<code>av-log {all disable novirus}</code>	Antivirus log settings. Select one of the following: <ul style="list-style-type: none"> <code>all</code>: Log all virus lookups. <code>disable</code>: Disable virus log. <code>novirus</code>: Log non-virus events.
<code>av-preload {disable enable}</code>	Enable/disable preloading the antivirus database into memory.
<code>eventlog-query {disable enable}</code>	Enable/disable record query to event-log besides fgdl-log.
<code>fq-cache <integer></code>	Set the file query service maximum memory usage (100 to 500MB).
<code>fq-log {all disable nofilequery}</code>	File query log settings. Select one of the following: <ul style="list-style-type: none"> <code>all</code>: Log all file query. <code>disable</code>: Disable file query log. <code>nofilequery</code>: Log non-file query events.
<code>fq-preload {disable enable}</code>	Enable/disable preloading the filequery database to memory.
<code>linkd-log {disable enable}</code>	Enable/disable the <code>linkd</code> log.
<code>max-log-quota <integer></code>	Maximum log quota setting (100-20480MB).
<code>max-unrated-size <integer></code>	Maximum number of unrated site in memory, from 10 to 5120K. The default is 500K.
<code>restrict-as1-dbver <string></code>	Restrict the system update to indicated the antispam (1) database version.

Variable	Description
<code>restrict-as2-dbver <string></code>	Restrict the system update to indicated the antispyam (2) database version.
<code>restrict-as4-dbver <string></code>	Restrict the system update to indicated the antispyam (4) database version.
<code>restrict-av-dbver <string></code>	Restrict the system update to indicated the antivirus database version.
<code>restrict-fq-dbver <string></code>	Restrict the system update to indicated filequery database version.
<code>restrict-wf-dbver <string></code>	Restrict the system update to indicated the webfilter database version.
<code>stat-log-interval <integer></code>	Statistic log interval setting (1-1440 minutes).
<code>stat-sync-interval <integer></code>	Synchronization interval for statistics of unrated sites, from 1 to 60 minutes.
<code>update-interval <integer></code>	Set the FortiGuard database update wait time if there are not enough delta files (2 to 24 hours).
<code>update-log {disable enable}</code>	Enable/disable update log setting.
<code>wf-cache <integer></code>	Set the web filter service maximum memory usage (100 to 2800MB).
<code>wf-log {all disable nouri}</code>	Web filter log setting. Select one of the following: <ul style="list-style-type: none"> <code>all</code>: Log all URL lookups. <code>disable</code>: Disable URL log. <code>nouri</code>: Log non-URL events.
<code>wf-preload {disable enable}</code>	Enable/disable preloading the web filter database into memory.

web-spam fgt server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard spam updates for FortiGate from the FDS.

Syntax

```
config fmupdate web-spam fgt server-override
  set status {enable | disable}
  config servlist
    edit <id>
      set ip <ipv4_address>
      set port <port_int>
```

```

end
end

```

Variable	Description
status {enable disable}	Enable/disable the override. Default: disable
Variables for config servlist subcommand:	
<id>	Override server ID (1-10).
ip <ipv4_address>	Enter the IPv4 address of the override server address. Default: 0.0.0.0
port <port_int>	Enter the port number to use when contacting the FDS. Default: 443

web-spam fsa server-override

Use this command to override the default IP address and port that the built-in FDS contacts when requesting FortiGuard spam updates for FortiSandbox from the FDS.

Syntax

```

config fmupdate web-spam fsa server-override
  set status {enable | disable}
  config servlist
    edit <id>
      set ip <ipv4_address>
      set port <port_int>
    end
  end
end

```

Variable	Description
status {enable disable}	Enable/disable the override. Default: disable
Variables for config servlist subcommand:	
<id>	Override server ID (1-10).
ip <ipv4_address>	Enter the IPv4 address of the override server address. Default: 0.0.0.0
port <port_int>	Enter the port number to use when contacting the FDS. Default: 443

web-spam poll-frequency

Use this command to configure the web-spam poll frequency.

Syntax

```

config fmupdate web-spam poll-frequency

```

```

    set time <hh:mm>
end

```

Variable	Description
time <hh:mm>	Enter the poll frequency time interval

web-spam web-proxy

Use this command to configure the web-spam web-proxy.

Syntax

```

config fmupdate web-spam web-proxy
    set time <hh:mm>
    set ip <ipv4_address>
    set mode {proxy | tunnel}
    set password <password_string>
    set port <integer>
    set status {disable | enable}
end

```

Variable	Description
ip <ipv4_address>	Enter the IPv4 address of the web proxy. Default: 0.0.0.0
mode {proxy tunnel}	Enter the web proxy mode. Select one of the following: <ul style="list-style-type: none"> proxy: HTTP proxy. tunnel: HTTP tunnel.
password <password_string>	If the web proxy requires authentication, enter the password for the user name.
port <integer>	Enter the port number of the web proxy. Default: 80
status {disable enable}	Enable/disable connections through the web proxy. Default: disable
username <string>	If the web proxy requires authentication, enter the user name.

execute

The `execute` commands perform immediate operations on your device. You can:

- Back up and restore the system settings, or reset the unit to factory settings.
- Set the unit date and time.
- Use ping to diagnose network problems.
- View the processes running on the FortiManager unit.
- Start and stop the FortiManager unit.
- Reset or shut down the FortiManager unit.



CLI commands and variables are case sensitive.

add-vm-license

Add a VM license to the FortiManager VM.

Syntax

```
execute add-vm-license <vm license>
```



This command is only available on FortiManager VM models.

backup

Use this command to backup the configuration or database to a file.

When you back up the unit settings from the `vdom_admin` account, the backup file contains global settings and the settings for each VDOM. When you back up the unit settings from a regular administrator account, the backup file contains the global settings and only the settings for the VDOM to which the administrator belongs.

Syntax

```
execute backup all-settings {ftp | scp | sftp} <ip> <string> <username> <password_string>
    <ssh-cert> <crtpasswd>
execute backup logs <device name(s)> {ftp | scp | sftp} <ip> <username> <password_string>
    <directory>
execute backup logs-only <device name(s)> {ftp | scp | sftp} <ip> <username> <password_
    string> <directory>
execute backup logs-rescue <device serial number(s)> {ftp | scp | sftp} <ip> <username>
    <password_string> <directory>
execute backup reports <report schedule name(s)> {ftp | scp | sftp} <ip> <username>
    <password_string> <directory>
```

```
execute backup reports-config <adom name(s)> {ftp | scp | sftp} <ip> <username> <password_string> <directory>
```

Variable	Description
all-settings	Backup all settings to a file on a server.
logs	Backup the device logs to a specified server.
logs-only	Backup device logs only to a specified server.
logs-rescue	Use this hidden command to backup logs regardless of DVM database for emergency reasons. This command will scan folders under /Storage/Logs/ for possible device logs to backup.
reports	Backup the reports to a specified server.
reports-config	Backup reports configuration to a specified server.
<device name(s)>	Enter the device name(s) separated by a comma, or enter <code>all</code> for all devices.
<device serial number(s)>	Enter the device serial number(s) separated by a comma, or enter <code>all</code> for all devices.
<report schedule name(s)>	Enter the report schedule name(s) separated by a comma, or enter <code>all</code> for all reports schedules.
<adom name(s)>	Enter the ADOM name(s) separated by a comma, or enter <code>all</code> for all ADOMs.
{ftp scp sftp}	Enter the server type.
<ip>	Enter the server IP address.
<string>	Enter the path and file name for the backup.
<username>	Enter username to use to log on the backup server.
<password_string>	Enter the password for the username on the backup server.
<ssh-cert>	Enter the SSH certification for the server. This option is only available for backup operations to SCP servers.
<crptpasswd>	Optional password to protect backup content. Use <code>any</code> for no password.
<directory>	Enter the path to where the file will be backed up to on the backup server.

Example

This example shows how to backup the system settings to a file named `fmg.cfg` on a server at IP address 192.168.1.23 using the admin username, a password of 123456.

```
execute backup all-settings ftp 192.168.1.23 fmd.cfg admin 123456
Starting backup all settings...
Starting transfer the backup file to FTP server...
```

bootimage

Use this command to set the boot image partition.

Syntax

```
execute bootimage <primary | secondary>
```



This command is only available on hardware models.

certificate

Use these commands to manage certificates.

certificate ca

Use these commands to list CA certificates, and to import or export CA certificates.

Syntax

To list the CA certificates installed on your device:

```
execute certificate ca list
```

To export or import CA certificates:

```
execute certificate ca {<export>|<import>} <cert_name> <tftp_ip>
```

Variable	Description
<export>	Export CA certificate to TFTP server.
<import>	Import CA certificate from a TFTP server.
list	Generate a list of CA certificates on your device.
<cert_name>	Name of the certificate.
<tftp_ip>	IP address of the TFTP server.

certificate local

Use these commands to list local certificates, and to import or export local certificates.

Syntax

To list the local certificates installed on your device:

```
execute certificate local list
```

To export or import local certificates:

```
execute certificate local {<export>|<import>} <cert_name> <tftp_ip>
```

Variable	Description
<export>	Export CA certificate to TFTP server.
<import>	Import CA certificate from a TFTP server.
list	Generate a list of CA certificates on your device.
<cert_name>	Name of the certificate.
<tftp_ip>	IP address of the TFTP server.

certificate local generate

Use this command to generate a certificate request.

Syntax

```
execute certificate local generate <certificate-name_str> <subject> <number>  
[<optional_information>]
```

Variable	Description
<certificate-name_str>	Enter a name for the certificate. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed.
<number>	Enter 512, 1024, 1536, or 2048 for the size, in bits, of the encryption key.
<subject>	Enter one of the following pieces of information to identify the FortiManager unit being certified: <ul style="list-style-type: none">the FortiManager unit IP addressthe fully qualified domain name of the FortiManager unitan email address that identifies the FortiManager unitAn IP address or domain name is preferable to an email address.

Variable	Description
[<optional_information>]	Enter <code>optional_information</code> as required to further identify the unit. You must enter the optional variables in the order that they are listed in the table. To enter any optional variable you must enter all of the variables that come before it in the list. For example, to enter the <code>organization_name_str</code> , you must first enter the <code>country_code_str</code> , <code>state_name_str</code> , and <code>city_name_str</code> . While entering optional variables, you can type? for help on the next required variable.

Optional information variables

Variable	Description
<country_code_str>	Enter the two-character country code.
<state_name_str>	Enter the name of the state or province where the FortiManager unit is located.
<city_name_str>	Enter the name of the city, or town, where the person or organization certifying the FortiManager unit resides.
<organization-name_str>	Enter the name of the organization that is requesting the certificate for the FortiManager unit.
<organization-unit_name_str>	Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiManager unit.
<email_address_str>	Enter a contact email address for the FortiManager unit.
<ca_server_url>	Enter the URL of the CA (SCEP) certificate server that allows auto-signing of the request.
<challenge_password>	Enter the challenge password for the SCEP certificate server.

chassis

Use this command to replace a chassis device password on your device.

Syntax

```
execute chassis replace <pw>
```

Variable	Description
<pw>	Replace the chassis password.



This command is only available on devices that support chassis management.

console baudrate

Use this command to get or set the console baudrate.

Syntax

```
execute console baudrate [9600 | 19200 | 38400 | 57600 | 115200]
```

If you do not specify a baudrate, the command returns the current baudrate.

Setting the baudrate will disconnect your console session.

Example

Get the baudrate:

```
execute console baudrate
```

The response is displayed:

```
current baud rate is: 115200
```

Set the baudrate to 9600:

```
execute console baudrate 9600
```

date

Get or set the system date.

Syntax

```
execute date [<date_str>]
```

`date_str` has the form `mm/dd/yyyy`, where

- `mm` is the month and can be 01 to 12
- `dd` is the day of the month and can be 01 to 31
- `yyyy` is the year and can be 2001 to 2100

If you do not specify a date, the command returns the current system date.

Dates entered will be validated - `mm` and `dd` require 2 digits, and `yyyy` requires 4 digits. Entering fewer digits will result in an error.

Example

This example sets the date to 17 September 2014:

```
execute date 09/17/2014
```

device

Use this command to change a device password or serial number when changing devices due to a hardware issue.

Syntax

```
execute device replace pw <name> <pw>
execute device replace sn <devname> <serialnum>
```

Variable	Description
<name>	The name of the device.
<pw>	The device password.
<devname>	The name of the device.
<serialnum>	The new serial number.

Example

```
execute device replace pw FGT600C2805030002
This operation will clear the password of the device.
Do you want to continue? (y/n)y
```

dmserver

Use these commands to manage devices and revisions.

dmserver delrev

Use this command to delete configuration revisions. The device name will be kept.

Syntax

```
execute dmserver delrev <device_name> <startrev> <endrev>
```

Variable	Description
<device_name>	The name of the device.
<startrev>	The starting configuration revision number that you want to delete.
<endrev>	The ending configuration revision number that you want to delete.

dmserver revlist

Use this command to show a list of revisions for a device.

Syntax

```
execute dmserver revlist <devicename>
```

Variable	Description
<devicename>	The name of the device.

dmserver showconfig

Use this command to show a specific configuration type and revision. You cannot use this command with read-only permission.

Syntax

```
execute dmserver showconfig <devicename>
```

Variable	Description
<devicename>	The name of the device.

dmserver showdev

Use this command to show a list of available devices. For each listed device, this command lists the device ID, device name, and serial number.

Syntax

```
execute dmserver showdev
```

dmserver showrev

Use this command to display a device's configuration revision. You cannot use this command with read-only permission.

Syntax

```
execute dmserver showrev <devicename> <revision>
```

Variable	Description
<devicename>	The name of the device.
<revision>	The configuration revision you want to display.

factory-license

Use this command to enter a factory license key. This command is hidden.

Syntax

```
execute factory-license <key>
```

Variable	Description
<key>	Enter the factory license key.

fgfm reclaim-dev-tunnel

Use this command to reclaim a management tunnel. The device name is optional.

Syntax

```
execute fgfm reclaim-dev-tunnel <devicename>
```

Variable	Description
<devicename>	Enter the device name.

fmpolicy

Use these commands to perform policy and object related actions.

fmpolicy check-upgrade-object

Use this command to check/upgrade objects by syntax.

Syntax

```
execute fmpolicy check-upgrade-object <action> {checking | fixing} <mode> <issue>
execute fmpolicy check-upgrade-object dump log
execute fmpolicy check-upgrade-object upload-log <ftpserver> <port> <path> <username>
<passwd>
```

Variable	Description
<action>	Select the auto-upgrade action. The following options are available: <ul style="list-style-type: none">• manual: Run auto-upgrade manually.• dump-log: Dump a detail log (size 8 K) on console.• upload-log: Upload a detail log (size 8 K) to a remote FTP server.
{checking fixing}	Select the action to take. The following options are available: <ul style="list-style-type: none">• checking: Only check for target issues.• fixing: Check for and then fix target issues.

Variable	Description
<mode>	Enter the mode. The following options are available: <ul style="list-style-type: none"> • basic: Only check/fix basic know cases. • auto: Only check/fix auto syntax based cases. • misc: Only check/fix misc know cases. • all: Check/fix all basic, auto, misc cases.
<issue>	Enter the ID, UUID, or enter all to fix all issues.
<ftpserver>	Enter the FTP server IP address. This option is available when <code>action</code> is <code>upload-log</code> .
<port>	Enter the FTP server port. This option is available when <code>action</code> is <code>upload-log</code> .
<path>	Enter the FTP server destination path. This option is available when <code>action</code> is <code>upload-log</code> .
<username>	Enter the FTP server username. This option is available when <code>action</code> is <code>upload-log</code> .
<password>	Enter the FTP server password. This option is available when <code>action</code> is <code>upload-log</code> .

fmpolicy copy-adom-object

Use this command to set the policy to copy an ADOM level object.

Syntax

```
execute fmpolicy copy-adom-object <adom> <category> <name> <devname> <vdom>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<category>	Enter the name of the category in the ADOM.
<name>	Enter the name of the object.
<devname>	Enter the name of the device.
<vdom>	Enter the name of the VDOM.

fmpolicy install-config

Use this command to print the configuration for an ADOM.

Syntax

```
execute fmpolicy install-config <adom> <devname> <revname>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<devname>	Enter the device name.
<revname>	Enter the install revision name.

fmpolicy print-adom-database

Use this command to print the ADOM database configuration.

Syntax

```
execute fmpolicy print-adom-database <adom> <output>
```

Variable	Description
<adom>	Enter the name of the ADOM or Global..
<output>	Enter the output file name.

fmpolicy print-adom-object

Use this command to print the ADOM object database.

Syntax

```
execute fmpolicy print-adom-object <adom> <category name> {<object name> | all | list}  
<output>
```

Variable	Description
<adom>	Enter the name of the ADOM or Global.
<category name>	Enter the category name.
{<object name> all list}	Show object by name. Enter <code>all</code> to show all objects, or enter <code>list</code> to get all objects.
<output>	Enter the output file name.

fmpolicy print-adom-package

Use this command to print the ADOM policy package database.

Syntax

```
execute fmpolicy print-adom-package <adom> <package name> <category name> {<object name> |
all | list} <output>
```

Variable	Description
<adom>	Enter the name of the ADOM or Global.
<package name>	Enter the package name.
<category name>	Enter the category name.
{<object name> all list}	Show object by name. Enter <code>all</code> to show all objects, or enter <code>list</code> to get all objects.
<output>	Enter the output file name.

fmpolicy print-device-database

Use this command to print the device database configuration for an ADOM.

Syntax

```
execute fmpolicy print-device-database <adom> <devname> <output>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<devname>	Enter the device name.
<output>	Enter the output filename.

fmpolicy print-device-object

Use this command to print the device objects.

Syntax

```
execute fmpolicy print-device-object <devname> <vdom> <category> {<object
name>|all|list} <output>
```

Variable	Description
<devname>	Enter the name of the device.
<vdom>	Enter the name of the VDOM.
<category>	Enter the category of the ADOM.

Variable	Description
{<object name> all list}	Show object by name. Enter <code>all</code> to show all objects, or enter <code>list</code> to get all objects.
<output>	Output file name.

fmprofile print-prov-templates

Use this command to print provisioning templates.

Syntax

```
execute fmprofile print-prov-templates <adom> <package name> <category name> {<object name> | all | list} <output>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<package name>	Enter the template name.
<category name>	Enter the category name.
{<object name> all list}	Show object by name. Enter <code>all</code> to show all objects, or enter <code>list</code> to get all objects.
<output>	Enter the output name.

fmprofile

Use these commands to perform profile related actions.

fmprofile copy-to-device

Use this command to copy profile settings from a profile to a device.

Syntax

```
execute fmprofile copy-to-device <adom> <profile-id> <devname>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<profile-id>	Enter the profile ID.
<devname>	Enter the device ID.

fmprofile export-profile

Use this command to export profile configurations.

Syntax

```
execute fmprofile export-profile <adom> <profile-id> <output>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<profile-id>	Enter the profile ID.
<output>	Enter the output file name.

fmprofile import-from-device

Use this command to import profile settings from a device to a profile.

Syntax

```
execute fmprofile import-from-device <adom> <devname> <profile-id>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<devname>	Enter the device ID.
<profile-id>	Enter the profile ID.

fmprofile import-profile

Use this command to import profile configurations.

Syntax

```
execute fmprofile import-profile <adom> <profile-id> <filename>
```

Variable	Description
<adom>	Enter the name of the ADOM.
<profile-id>	Enter the profile ID.
<filename>	Enter the full path to the input file containing CLI configuration.

fmprofile list-profiles

Use this command to list all profiles in an ADOM.

Syntax

```
execute fmprofile list-profiles <adom>
```

Variable	Description
<adom>	Enter the name of the ADOM.

fmscript

Use these commands to perform script related actions.

fmscript clean-sched

Clean the script schedule table for all non-exist devices.

Syntax

```
execute fmscript clean-sched
```

fmscript delete

Delete a script from FortiManager.

Syntax

```
execute fmscript delete <scriptid>
```

Variable	Description
<scriptid>	The name of the script to delete.

fmscript import

Import a script from an FTP server to FortiManager.

Syntax

```
execute fmscript import <ftpserver_ipv4> <filename> <username> <password> <scriptname>  
    <scripttype> <comment> <adom_name> <os_type> <os_version> <platform> <devicename>  
    <buildno> <hostname> <serialno>
```

Variable	Description
<ftpserver_ipv4>	The IP address of the FTP server.
<filename>	The filename of the script to be imported to the system.
<username>	The user name used to access the FTP server.
<password>	The password used to access the FTP server.

Variable	Description
<scriptname>	The name of the script to import.
<scripttype>	The type of script as one of CLI or TCL.
<comment>	A comment about the script being imported, such as a brief description.
<adom_name>	Name of the administrative domain.
<os_type>	The operating system type, such as FortiOS. Options include <i>any</i> , <i>FortiOS</i> , and others.
<os_version>	The operating system version, such as FortiOS. Options include <i>any</i> , 400, and 500.
<platform>	The hardware platform this script can be run on. Options include <i>any</i> , or the model of the device such as <i>Fortigate 60C</i> .
<devicename>	The device name to run this script on. Options include <i>any</i> , or the specific device name as it is displayed on the FortiManager system
<buildno>	The specific build number this script can be run on. Options include <i>any</i> , or the three digit build number. Build numbers can be found in the firmware name for the device.
<hostname>	The host name of the device this script can be run on. Options include <i>any</i> , or the specific host name.
<serialno>	The serial number of the device this script can be run on. Options include <i>any</i> , or the specific serial number of the device, such as <i>FGT60C3G28033042</i> .

fmscript list

List the scripts on the FortiManager device.

Syntax

```
execute fmscript list
```

Example

This is a sample output of the `execute fmscript list` command.

```
FMG400C # execute fmscript list
scriptid=8,name=new account profile,type=CLI
scriptid=7,name=import_script,type=CLI
scriptid=6,name=group1,type=CLIGROUP
scriptid=5,name=basic_test,type=CLI
scriptid=3,name=interface info,type=CLI
scriptid=1,name=xml_script1,type=CLI
```

fmscript run

Run a script on a device, the device's object database, or on the global database. Only CLI scripts can be run on databases, and they must contain only complete commands. Any scripts that use shortened CLI commands will generate errors.

When a script is run on the database, the device will be updated with any configuration changes the next time the configuration is uploaded from the FortiManager system to the device.

Syntax

```
execute fmscript run <scriptid_int> <run_on> <devname> <adomname>
```

Variable	Description
<scriptid_int>	The ID number of the script to run.
<run_on>	Select where to run the script: <ul style="list-style-type: none"> device: on the device group: on a group devicedb: on the device's object database globaldb: on the global database
<devname>	Enter the device name to run the script on. This is required if device or devicedb were chosen for where to run the script.
<adomname>	Name of the administrative domain.

fmscript showlog

Display the log of scripts that have run on the selected device.

Syntax

```
execute fmscript showlog <devicename>
```

Variable	Description
<devicename>	The name of a managed FortiGate device.

Example

This example shows the output of `execute fmscript showlog Dev3` that displays the output from a CLI script called `xml_script1` that was run on the object database.

```
execute fmscript showlog Dev3
Starting log
config firewall address
  edit 33
    set subnet 33.33.33.33 255.255.255.0
config firewall address
  edit 33
```

```
Running script(xml_script1) on DB success
cdb_find_entry_by_canon,52:parent=1,category=2,key=(null)
```

fmupdate

Use these commands to import and export packages.

fmupdate {ftp | scp | tftp} import

You can import packages using the FTP, SCP, or TFTP servers. You can use this command to import a list of custom URLs. Use the `custom-url-list` command to configure the URL database that FortiManager will use for rating queries.

Syntax

```
execute fmupdate {ftp | scp | tftp} import <type> <remote_file> <ip> <port> <remote_path> <user> <password_string>
```

Variable	Description
{ftp scp tftp}	Select ftp, scp, or tftp as the file transfer protocol to use.
<type>	Select the type of file to export or import. Options include: av-ips, fct-av, url, spam, file-query, license-fgt, license-fct, custom-url, and domp.
<remote_file>	Update manager packet file name on the server or host.
<ip>	Enter the FQDN or the IP address of the server.
<port>	Enter the port to connect to on the remote SCP host.
<remote_path>	Enter the name of the directory of the file to download from the FTP server or SCP host. If the directory name has spaces, use quotes instead.
<user>	Enter the user name to log into the FTP server or SCP host
<password_string>	Enter the password to log into the FTP server or SCP host

fmupdate {ftp | scp | tftp} export

You can export packages using the FTP, SCP, or TFTP servers.

Syntax

```
execute fmupdate {ftp | scp | tftp} export <type> <remote_file> <ip> <port> <remote_path> <user> <password>
```

Variable	Description
{ftp scp tftp}	Select ftp, scp, or tftp as the file transfer protocol to use.
<type>	Select the type of file to export or import. Options include: url, spam, license-package, license-info-in-xml, custom-url, and domp.
<remote_file>	Update manager packet file name on the server or host.
<ip>	Enter the FQDN or the IPv4 address of the server.
<port>	Enter the port to connect to on the remote SCP host.
<remote_path>	Enter the name of the directory of the file to download from the FTP server or SCP host. If the directory name has spaces, use quotes instead.
<user>	Enter the user name to log into the FTP server or SCP host
<password>	Enter the password to log into the FTP server or SCP host

format

Format the hard disk on the FortiManager system.

Syntax

```
execute format <disk | disk-ext4> <RAID level>
```

When you run this command, you will be prompted to confirm the request.



Executing this command will erase all device settings/images, VPN & Update Manager databases, and log data on the FortiManager system's hard drive. The FortiManager device's IP address, and routing information will be preserved.

Variable	Description
<disk disk-ext4>	Select to format the hard disk or format the hard disk with ext4 file system.
<disk_partition_2>	Format hard disk partition 2 (static)
<disk_partition_2-ext4>	Format hard disk partition 2 (static) with ext4 file system.
<disk_partition_3>	Format hard disk partition 3 (dynamic)

Variable	Description
<disk_partition_3-ext4>	Format hard disk partition 3 (dynamic) with ext4 file system.
<disk_partition_4>	Format hard disk partition 4 (misc)
<disk_partition_4-ext4>	Format hard disk partition 4 (misc) with ext4 file system.
<RAID level>	Enter the RAID level to be set on the device. This option is only available on FortiManager models that support RAID. Press the Enter key to show available RAID levels.

log

Use these commands to manage device logs.

log device disk_quota

Set the log device disk quota.

Syntax

```
execute log device disk_quota <device_id> <value>
```

Variable	Description
<device_id>	Enter the log device ID number, or All for all devices.
<value>	Enter the disk quota value, in MB.

log device permissions

Set or view the log device permissions.

Syntax

```
execute log device permissions <device_id> <permission> {enable | disable}>
```

Variable	Description
<device_id>	Enter the log device ID number, or All for all devices.

Variable	Description
<permission>	Select one of the following: <ul style="list-style-type: none"> all: All permissions logs: Log permission content: Content permission quar: Quarantine permission ips: IPS permission
{enable disable}>	Enable/disable the option.

log dlp-files clear

Delete log DLP files.

Syntax

```
execute log dlp-files clear <string> <string>
```

Variable	Description
<string>	Enter the device name.
<string>	Enter the device archive type. Select one of: all, email, im, ftp, http, or mms.

log import

Use this command to import log files from another device and replace the device ID on imported logs.

Syntax

```
execute log import <service> <ipv4_address> <user-name> <password_string> <file-name> <device-id>
```

Variable	Description
<service>	Enter the transfer protocol. Select one of: ftp, sftp, scp, or tftp.
<ipv4_address>	Enter the server IPv4 address.
<user-name>	Enter the username.
<password_string>	Enter the password or – for no password. The <password> field is not required when <service> is tftp.
<file-name>	The file name (e.g. dir/fgt.alog.log) or directory name (e.g. dir/subdir/).
<device-id>	Replace the device ID on imported logs. Enter a device serial number of one of your log devices. For example, FG100A2104400006.

log ips-pkt clear

Delete IPS packet files.

Syntax

```
execute log ips-pkt clear <string>
```

Variable	Description
<string>	Enter the device name.

log quarantine-files clear

Delete log quarantine files.

Syntax

```
execute log quarantine-files clear ><string>
```

Variable	Description
<string>	Enter the device name.

log-integrity

Query the log file's MD5 checksum and timestamp.

Syntax

```
execute log-integrity <device name> <string>
```

Variable	Description
<device name>	Enter the name of the log device. Example: FWF40C3911000061
<string>	The log file name

lvm

With Logical Volume Manager (LVM), a FortiManager VM device can have up to twelve total log disks added to an instance. More space can be added by adding another disk and running the LVM extend command.



This command is only available on FortiManager VM models.

Syntax

```
execute lvm extend [arg...]  
execute lvm info  
execute lvm start
```

Variable	Description
extend	Extend the LVM logical volume.
[arg...]	Argument list (0 to 11).
info	Get system LVM information.
start	Start using LVM.

Example

View LVM information:

```
execute lvm info  
disk01 In use 80.0 (GB)  
disk02 Not present  
disk03 Not present  
disk04 Not present  
disk05 Not present  
disk06 Not present  
disk07 Not present  
disk08 Not present  
disk09 Not present  
disk10 Not present  
disk11 Not present  
disk12 Not present
```

ping

Send an ICMP echo request (ping) to test the network connection between the FortiManager system and another network device.

Syntax

```
execute ping {<ipv4_address> | <hostname>}
```

Variable	Description
<ipv4_address>	IPv4 address of network device to contact.
<hostname>	DNS resolvable hostname of network device to contact.

Example

This example shows how to ping a host with the IP address 192.168.1.23:

```
execute ping 192.168.1.23
```

ping6

Send an ICMP echo request (ping) to test the network connection between the FortiManager system and another network device.

Syntax

```
execute ping6 {<ipv6_address> | <hostname>}
```

Variable	Description
<ipv6_address>	IPv6 address of network device to contact.
<hostname>	DNS resolvable hostname of network device to contact.

Example

This example shows how to ping a host with the IP address 8001:0DB8:AC10:FE01:0:0:0:0:

```
execute ping6 8001:0DB8:AC10:FE01:0:0:0:0:
```

raid

Use these commands to add or delete a hard disk to RAID.

Syntax

```
execute raid add-disk <disk index>  
execute raid delete-disk <disk index>
```



This command is only available on FortiManager models that support RAID.

reboot

Restart the FortiManager system. This command will disconnect all sessions on the FortiManager system.

Syntax

```
execute reboot
```

Example

```
execute reboot  
The system will be rebooted.  
Do you want to continue? (y/n)
```

remove

Use this command to remove all reports for a specific device from the FortiManager system.

Syntax

```
execute remove <reports> <device-id>
```

Variable	Description
<reports>	Remove all reports.
<device-id>	Enter the device identifier

Example

```
execute remove reports FGT60C3G000000002
This operation will ERASE ALL reports that include FGT60C3G000000002!
Do you want to continue? (y/n)y

All reports that include FGT60C3G000000002 were removed.
```

reset

Use this command to reset the FortiManager unit to factory defaults. This command will disconnect all sessions and restart the FortiManager unit.

Syntax

```
execute reset all-settings
```

Example

```
execute reset all-settings
This operation will reset all settings to factory defaults
Do you want to continue? (y/n)
```

reset-sqllog-transfer

Use this command to resend SQL logs to the database.

Syntax

```
execute reset-sqllog-transfer <enter>
```

restore

Use these commands to:

- restore the configuration or database from a file
- change the FortiManager unit image

This command will disconnect all sessions and restart the FortiManager unit

Syntax

```
execute restore all-settings {ftp | scp | sftp} <ip> <string> <username> <password_
string> <ssh-cert> <crtpassword_string> [option1+option2+...]
execute restore image {ftp | tftp} <filepath> <ip> <username> <password_string>
execute restore logs <device name(s)> {ftp | scp | sftp} <ip> <username> <password_
string> <directory>
execute restore logs-only <device name(s)> {ftp | scp | sftp} <ip> <username>
<password_string> <directory>
execute restore reports <report schedule name(s)> {ftp | scp | sftp} <ip> <username>
<password_string> <directory>
execute restore reports-config <adom name(s)> {ftp | scp | sftp} <ip> <username>
<password_string> <directory>
```

Variable	Description
all-settings	Restore all FortiManager settings from a file on a server. The new settings replace the existing settings, including administrator accounts and passwords.
image	Upload a firmware image from a TFTP server to the FortiManager unit. The FortiManager unit reboots, loading the new firmware.
logs	Restore the device logs.
logs-only	Restore only the device logs.
reports	Restore device reports.
reports-config	Restore the reports configuration.
{ftp tftp}	Enter the type of server to retrieve the image from.
{ftp scp sftp}	Enter the type of server.
<device name(s)>	Enter the device name(s) separated by a comma, or enter <code>all</code> for all devices.
<report schedule name(s)>	Enter the report schedule name(s) separated by a comma, or enter <code>all</code> for all reports schedules.

Variable	Description
<adom name(s)>	Enter the ADOM name(s) separated by a comma, or enter <code>all</code> for all ADOMs.
<filepath>	The file to get from the server. You can enter a path with the file-name, if required.
<ip>	IP address of the server to get the file from.
<string>	The file to get from the server. You can enter a path with the file-name, if required.
<username>	The username to log on to the server. This option is not available for restore operations from TFTP servers.
<password_string>	The password for username on the server. This option is not available for restore operations from TFTP servers.
<ssh-cert>	The SSH certification for the server. This option is only available for restore operations from SCP servers.
<crptpassword_string>	Optional password to protect backup content. Use <code>any</code> for no password.
<directory>	Enter the directory.
[option1+option2+...]	Select whether to keep IP, routing, and HA info on the original unit.

Example

This example shows how to upload a configuration file from a FTP server to the FortiManager unit. The name of the configuration file on the FTP server is `backupconfig`. The IP address of the FTP server is `192.168.1.23`. The user is `admin` with a password of `mypassword`. The configuration file is located in the `/usr/local/backups/` directory on the TFTP server.

```
execute restore all-settings 192.168.1.23 /usr/local/backups/backupconfig admin
mypassword
```

shutdown

Shut down the FortiManager system. This command will disconnect all sessions.

Syntax

```
execute shutdown
```

Example

```
execute shutdown
The system will be halted.
```

Do you want to continue? (y/n)

sql-local

Use these commands to remove the SQL database and logs from the FortiManager system and to rebuild the database and devices.



When rebuilding the SQL database, new logs will not be available until the rebuild is complete. The time required to rebuild the database is dependent on the size of the database. Please plan a maintenance window to complete the database rebuild. You can use the `diagnose sql status rebuild-db` command to display the SQL log database rebuild status.

sql-local rebuild-db

Syntax

```
execute sql-local <rebuild-db>
```

Variable	Description
<rebuild-db>	Rebuild the entire local SQL database.

sql-local remove-db

Syntax

```
execute sql-local <remove-db>
```

Variable	Description
<remove-db>	Remove entire local SQL database.

sql-local remove-logtype

Syntax

```
execute sql-local <remove-logtype> <log type>
```

Variable	Description
<remove-logtype>	Remove all log entries of the designated log type.
<log type>	Enter the log type from available log types. Example: <code>app-ctrl</code>

Example

```
execute sql-local remove-logtype app-ctrl
All SQL logs with log type 'app-ctrl' will be erased!
Do you want to continue? (y/n)
```

sql-query-dataset

Use this command to execute a SQL dataset against the system.

Syntax

```
execute sql-query-dataset <adom> <dataset-name> <device/group name> <faz/dev> <start-time>
<end-time>
```

Variable	Description
<adom>	Enter the ADOM name.
<dataset-name>	Enter the dataset name.
<device/group name>	Enter the name of the device or device group.
<faz/dev>	Enter the name of the FortiAnalyzer.
<start-time>	Enter the log start time.
<end-time>	Enter the log end time.

Example

```
execute sql-query-dataset Top-App-By-Bandwidth
```

sql-query-generic

Use this command to execute a SQL statement against the system.

Syntax

```
execute sql-query-generic <string>
```

Variable	Description
<string>	Enter the SQL statement to run.

sql-report

Use these commands to import and display language translation files and run a SQL report once against the FortiManager system.

sql-report hcache-check

Use this command to check the report hcache.

Syntax

```
execute sql-report hcache-check <adom> <report-name> <start-time> <end-time>
```

Variable	Description
<adom>	The ADOM name to run the report.
<report-name>	Enter the report name.
<start-time>	Enter the start date and time of the report schedule in the format HH:MM yyyy/mm/dd.
<end-time>	Enter the end date and time of the report schedule in the format HH:MM yyyy/mm/dd.

sql-report import-lang

Use this command to import a user defined language translation file.

Syntax

```
execute sql-report import-lang <name> <service> <ip> <argument 1> <argument 2> <argument 3>
```

Variable	Description
<name>	Enter the new language name to import a new language translation file.
<service>	Transfer protocol. Type one of the following: <ul style="list-style-type: none">• ftp: FTP• sftp: SFTP• scp: SCP• tftp: TFTP
<ip>	Server IP address.
<argument 1>	For FTP, SFTP, or SCP, enter a user name. For TFTP, enter a file name.
<argument 2>	For FTP, SFTP, or SCP, enter a password or '-'. For TFTP, press <enter>.

Variable	Description
<argument 3>	Enter a filename and press <enter>.

sql-report list

Use this command to list recent reports generated.

Syntax

```
execute sql-report list <adom> <days-range> <layout-name>
```

Variable	Description
<adom>	The name of the ADOM.
<days-range>	Enter the number of days. Range: 1 to 99
<layout-name>	Select one of the available SQL report layout names.

sql-report list-lang

Use this command to display all supported language translation files.

Syntax

```
execute sql-report list-lang
```

sql-report list-schedule

Use this command to list all report schedules.

Syntax

```
execute sql-report list-schedule <adom>
```

Variable	Description
<adom>	The name of the ADOM.

sql-report run

Use this command to run a report once.

Syntax

```
execute sql-report run <adom> <schedule-name> <num-threads>
```

Variable	Description
<name>	Enter the new language name to import a new language translation file.
<service>	Transfer protocol. Type one of the following: <ul style="list-style-type: none"> • ftp: FTP • sftp: SFTP • scp: SCP • tftp: TFTP
<ip>	Server IP address.
<argument 1>	For FTP, SFTP, or SCP, enter a user name. For TFTP, enter a file name.
<argument 2>	For FTP, SFTP, or SCP, enter a password or '-'. For TFTP, press <enter>.
<argument 3>	Enter a filename and press <enter>.
<adom>	The ADOM name to run the report.
<schedule-name>	Select one of the available report schedule names.
<num-threads>	Select the number of threads.

sql-report view

Use this command to view report data.

Syntax

```
execute sql-report view <data-type> <adom> <report-name>
```

Variable	Description
<data-type>	Enter the data type to view. For example "report-data".
<adom>	Enter the name of the ADOM.
<report-name>	Enter the name of the report to view.

ssh

Use this command to establish an SSH session with another system.

Syntax

```
execute ssh <destination> <username>
```

Variable	Description
<destination>	Enter the IP address or FQ DNS resolvable hostname of the system you are connecting to.
<username>	Enter the user name to use to log on to the remote system.

To leave the SSH session type `exit`.

To confirm you are connected or disconnected from the SSH session, verify the command prompt has changed.

ssh-known-hosts

Use these commands to remove all known SSH hosts.

Syntax

```
execute ssh-known-hosts remove-all
execute ssh-known-hosts remove-host <host/ip>
```

Variable	Description
<host/ip>	Enter the hostname or IP address of the SSH host to remove.

time

Get or set the system time.

Syntax

```
execute time [<time_str>]
time_str has the form hh:mm:ss, where
```

- `hh` is the hour and can be 00 to 23
- `mm` is the minutes and can be 00 to 59
- `ss` is the seconds and can be 00 to 59

All parts of the time are required. Single digits are allowed for each of `hh`, `mm`, and `ss`.

If you do not specify a time, the command returns the current system time.

```
execute time <enter>
current time is: 12:54:22
```

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

top

Use this command to view the processes running on the FortiManager system.

Syntax

execute top

Command	Description
Z,B	Global: 'z' change color mappings; 'B' disable/enable bold.
l,t,m	Toggle Summaries: 'l' load average; 't' task/cpu statistics; 'm' memory information.
1,l	Toggle SMP view: '1' single/separate states; 'I' Irix/Solaris mode.
f,o	Fields/Columns: 'f' add or remove; 'o' change display order.
F or O	Select sort field.
<,>	Move sort field: '<' next column left; '>' next column right.
R,H	Toggle: 'R' normal/reverse sort; 'H' show threads.
c,i,S	Toggle: 'c' command name/line; 'i' idle tasks; 'S' cumulative time.
x,y	Toggle highlights: 'x' sort field; 'y' running tasks.
z,b	Toggle: 'z' color/mono; 'b' bold/reverse (only if 'x' or 'y').
u	Show specific user only.
n or #	Set maximum tasks displayed.
k,r	Manipulate tasks: 'k' kill; 'r' renice.
d or s	Set update interval.
W	Write configuration file.
q	Quit

Example

The `execute top` command displays the following information:

```
top_bin - 12:50:25 up 1:48, 0 users, load average: 0.00, 0.02, 0.05
Tasks: 168 total, 1 running, 167 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.0%us, 0.0%sy, 0.0%ni,100.0%id, 0.0%wa, 0.0%hi, 0.0%si, 0.0%st
Mem: 6108960k total, 923440k used, 5185520k free, 24716k buffers
Swap: 2076536k total, 0k used, 2076536k free, 306136k cached
H
```

```

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
5566 root 20 0 187m 159m 4432 S 0 2.7 0:04.63 dmserver
13492 root 20 0 2072 956 708 R 0 0.0 0:00.01 top_bin
  1 root 20 0 186m 159m 5016 S 0 2.7 0:11.77 initXXXXXXXXXX
  2 root 20 0 0 0 0 S 0 0.0 0:00.00 kthreadd
  3 root 20 0 0 0 0 S 0 0.0 0:00.00 ksoftirqd/0
  4 root 20 0 0 0 0 S 0 0.0 0:00.00 kworker/0:0
  5 root 20 0 0 0 0 S 0 0.0 0:00.00 kworker/u:0
  6 root RT 0 0 0 0 S 0 0.0 0:00.00 migration/0
  7 root RT 0 0 0 0 S 0 0.0 0:00.00 migration/1
  8 root 20 0 0 0 0 S 0 0.0 0:00.00 kworker/1:0
  9 root 20 0 0 0 0 S 0 0.0 0:00.00 ksoftirqd/1
 10 root 20 0 0 0 0 S 0 0.0 0:00.18 kworker/0:1
 11 root RT 0 0 0 0 S 0 0.0 0:00.00 migration/2
 12 root 20 0 0 0 0 S 0 0.0 0:00.00 kworker/2:0
 13 root 20 0 0 0 0 S 0 0.0 0:00.00 ksoftirqd/2
 14 root RT 0 0 0 0 S 0 0.0 0:00.00 migration/3

```

traceroute

Test the connection between the FortiManager system and another network device, and display information about the network hops between the device and the FortiManager system.

Syntax

```
execute traceroute <host>
```

Variable	Description
<host>	IPv4 address or hostname of network device.

Example

This example shows how trace the route to a host with the IP address 172.18.4.95:

```

execute traceroute 172.18.4.95
traceroute to 172.18.4.95 (172.18.4.95), 32 hops max, 72 byte packets
1 172.18.4.95 0 ms 0 ms 0 ms
2 172.18.4.95 0 ms 0 ms 0 ms

```

traceroute6

Test the connection between the FortiManager system and another network device, and display information about the network hops between the device and the FortiManager system.

Syntax

```
execute traceroute6 <host>
```

Variable	Description
<host>	IPv6 address or hostname of network device.

Example

This example shows how trace the route to a host with the IPv6 address 8001:0DB8:AC10:FE01:0:0:0:0:

```
execute traceroute6 8001:0DB8:AC10:FE01:0:0:0:0
```

diagnose

The `diagnose` commands display diagnostic information that help you to troubleshoot problems.



CLI commands and variables are case sensitive.

auto-delete

Use this command to diagnose auto deletion of DLP files, log files, quarantine files, and report files.

Syntax

```
diagnose auto-delete dlp-files {delete-now | list}
diagnose auto-delete log-files {delete-now | list}
diagnose auto-delete quar-files {delete-now | list}
diagnose auto-delete report-files {delete-now | list}
```

Variable	Description
<code>dlp-files</code> {delete-now list}	Delete DLP files right now according to the system automatic deletion policy or list DLP files. Select one of the following: <ul style="list-style-type: none"><code>delete-now</code>: Delete files right now according to system automatic deletion policy.<code>list</code>: List files according to system automatic deletion policy.
<code>log-files</code> {delete-now list}	Delete log files right now according to the system automatic deletion policy or list log files. Select one of the following: <ul style="list-style-type: none"><code>delete-now</code>: Delete files right now according to system automatic deletion policy.<code>list</code>: List files according to system automatic deletion policy.
<code>quar-files</code> {delete-now list}	Delete quarantine files right now according to the system automatic deletion policy or list quarantine files. Select one of the following: <ul style="list-style-type: none"><code>delete-now</code>: Delete files right now according to system automatic deletion policy.<code>list</code>: List files according to system automatic deletion policy.
<code>report-files</code> {delete-now list}	Delete report files right now according to the system automatic deletion policy or list report files. Select one of the following: <ul style="list-style-type: none"><code>delete-now</code>: Delete files right now according to system automatic deletion policy.<code>list</code>: List files according to system automatic deletion policy.

cdb check

Use this command to check the object configuration database integrity, the global policy assignment table, and repair configuration database.

Syntax

```
diagnose cdb check objcfg-integrity
diagnose cdb check policy-assignment
diagnose cdb check reference-integrity
diagnose cdb check update-devinfo <item> <new-value> [0 | 1] [model-name]
```

Variable	Description
objcfg-integrity	Check object config database integrity.
policy-assignment	Check the global policy assignment table.
reference-integrity	Check the ADOM reference table integrity.
update-devinfo	Update device information by directly changing the database. <ul style="list-style-type: none"> • <item>: Device info item. • [new-value]: Item new value (Default sump summary only). • [0 1]: Choose one of: <ul style="list-style-type: none"> • 0: Only update empty value (default). • 1: Always update • [model-name]: Only update on model name. Default: all models.

Example

```
# diagnose cdb check policy-assignment
Checking global policy assignment ... correct
```

debug

Use the following commands to debug the FortiManager:

debug application

Use this command to set the debug levels for applications.

Syntax

```
diagnose debug application alertmail <integer>
diagnose debug application curl <integer>
diagnose debug application ddmd <integer> [deviceName]
diagnose debug application depmanager <integer>
```

```

diagnose debug application dmapi <integer>
diagnose debug application fazcfgd <integer>
diagnose debug application fazsvcd <integer>
diagnose debug application fgdsrv <integer>
diagnose debug application fgdupd <integer>
diagnose debug application fgfmsd <integer> [deviceName]
diagnose debug application fnbam <integer>
diagnose debug application fortilogd <integer>
diagnose debug application FortiManagerws <integer>
diagnose debug application gui <integer>
diagnose debug application ha <integer>
diagnose debug application ipsec <integer>
diagnose debug application localmod <integer>
diagnose debug application logd <integer>
diagnose debug application logfiled <integer>
diagnose debug application lrm <integer>
diagnose debug application ntpd <integer>
diagnose debug application oftpd <integer> [IP/deviceSerial/deviceName]
diagnose debug application ptmgr <integer>
diagnose debug application ptsessionmgr <integer>
diagnose debug application securityconsole <integer>
diagnose debug application snmpd <integer>
diagnose debug application sql_dashboard_rpt <integer>
diagnose debug application sql-integration <integer>
diagnose debug application sqlplugind <integer>
diagnose debug application sqlrptcached <integer>
diagnose debug application srchd <integer>
diagnose debug application ssh <integer>
diagnose debug application sshd <Integer>
diagnose debug application storaged <integer>
diagnose debug application uploadd <integer>

```

Variable	Description	Default
alertmail <integer>	Set the debug level of the alert email daemon.	0
curl <integer>	Set the debug level of the curl daemon. Use this CLI command to enable debug for monitoring progress when performing a backup/restore of a large database via FTP.	
ddmd <integer> [deviceName]	Set the debug level of the dynamic data monitor. Enter a device name to only show messages related to that device.	0
depmanager <integer>	Set the debug level of the deployment manager.	0
dmworker <Integer>	Set the debug level of the deployment manager worked.	
dmapi <integer>	Set the debug level of the dmapi.	0

Variable	Description	Default
fazcfgd <integer>	Set the debug level of the fazcfgd daemon.	0
fazsvcd <integer>	Set the debug level of the fazsvcd daemon.	0
fgdsvr <integer>	Set the debug level of the FortiGuard query daemon.	0
fgdupd <integer>	Set the debug level of the FortiGuard update daemon.	0
fgfmsd <integer> [deviceName]	Set the debug level of FGFM daemon. Enter a device name to only show messages related to that device.	0
fnbam <integer>	Set the debug level of the Fortinet authentication module.	0
fortilogd <integer>	Set the debug level of the fortilogd daemon.	0
FortiManagerws <integer>	Set the debug level of the Web Service.	0
gui <integer>	Set the debug level of the GUI.	0
ha <integer>	Set the debug level of high availability daemon.	0
ipsec <integer>	Set the debug level of the IPsec daemon.	0
localmod <integer>	Set the debug level of the localmod daemon.	0
logd <integer>	Set the debug level of the log daemon.	0
logfiled <integer>	Set the debug level of the logfiled daemon.	0
lrm <integer>	Set the debug level of the Log and Report Manager.	0
ntpd <integer>	Set the debug level of the NTP daemon.	0
oftpd <integer> [IP/deviceSerial/deviceName]	Set the debug level of the oftpd daemon. Enter an IP address, device serial number, or device name to only show messages related to that device or IP address.	0
ptmgr <integer>	Set the debug level of the Portal Manager.	0
ptsessionmgr <integer>	Set the debug level of the Portal Session Manager.	0

Variable	Description	Default
securityconsole <integer>	Set the debug level of the security console daemon.	0
snmpd <integer>	Set the debug level of the SNMP daemon from 0-8.	0
sql_dashboard_rpt <integer>	Set the debug level of the SQL dashboard report daemon.	0
sql-integration <integer>	Set the debug level of SQL applications.	0
sqlplugind <integer>	Set the debug level of the SQL plugin daemon.	0
sqlrptcached <integer>	Set the debug level of the SQL report caching daemon.	0
srchd <integer>	Set the debug level of the SRCHD.	0
ssh <integer>	Set the debug level of SSH protocol transactions.	0
sshd <Integer>	Set the debug level of the SSH daemon.	
storaged <integer>	Set the debug level of communication with java clients.	0
uploadd <integer>	Set the debug level of the upload daemon.	0

Example

This example shows how to set the debug level to 7 for the upload daemon:

```
diagnose debug application uploadd 7
```

debug cli

Use this command to set the debug level of CLI.

Syntax

```
diagnose debug cli <integer>
```

Variable	Description
<integer>	Set the debug level of the CLI from 0-8. Default: 3

Example

This example shows how to set the CLI debug level to 5:

```
diagnose debug cli 5
```

debug console

Use this command to enable or disable console debugging.

Syntax

```
diagnose debug console {enable | disable}
```

Variable	Description
{enable disable}	Enable/disable console debugging.

debug crashlog

Use this command to manage crash logs.

Syntax

```
diagnose debug crashlog clear
diagnose debug crashlog read
```

Variable	Description
clear	Delete backtrace and core files.
read	Show the crash logs. This command is hidden.

debug disable

Use this command to disable debug.

Syntax

```
diagnose debug disable
```

debug dpm

Use this command to manage the deployment manager.

Syntax

```
diagnose debug dpm comm-trace {enable | disable | status}
diagnose debug dpm conf-trace {enable | disable | status}
diagnose debug dpm probe-device <ip>
```

Variable	Description
comm-trace {enable disable status}	Enable a DPM to FortiGate communication trace. Type one of the following: <ul style="list-style-type: none"> enable: Enable communication trace. disable: Disable communication trace. status: Get the status of setting.
conf-trace {enable disable status}	Enable a DPM to FortiGate configuration trace. Type one of the following: <ul style="list-style-type: none"> enable: Enable configuration trace. disable: Disable configuration trace. status: Get the status of setting.
probe-device <ip>	Check device status.

Example

This example shows how to enable a communication trace between the DPM and a FortiGate:

```
diagnose debug dpm comm-trace enable
```

debug enable

Use this command to enable debug.

Syntax

```
diagnose debug enable
```

debug info

Use this command to show active debug level settings.

Syntax

```
diagnose debug info
```

Example

Here is an example of the output from `diagnose debug info`:

```
General
cli debug level: 3
console debug output: enable
debug timestamps: disable
terminal session debug output: disable

Application
ddmd debug filter: disable
fgfmsd debug filter: disable
oftpd debug filter: disable
```

debug reset

Use this command to reset the debug level settings. All debug settings will be reset.

Syntax

```
diagnose debug reset
```

debug service

Use this command to debug services.

Syntax

```
diagnose debug service cdb <integer>
diagnose debug service cmdb <integer>
diagnose debug service dvmcmd <integer>
diagnose debug service dvmdb <integer>
diagnose debug service fazconf <integer>
diagnose debug service main <integer>
diagnose debug service sys <integer>
diagnose debug service task <integer>
```

Variable	Description
cdb <integer>	Debug the CDB daemon service. Enter the debug level.
cmdb <integer>	Debug the CMDb daemon service. Enter the debug level.
dvmcmd <integer>	Debug the DVMCMD daemon service. Enter the debug level.
dvmdb <integer>	Debug the DVMDb daemon service. Enter the debug level.
fazconf <integer>	Debug the NCMDb daemon service. Enter the debug level.
main <integer>	Debug the Main daemon service. Enter the debug level.
sys <integer>	Debug the SYS daemon service. Enter the debug level.
task <integer>	Debug the Task daemon service. Enter the debug level.

debug sysinfo

Use this command to show system information.

Syntax

```
diagnose debug sysinfo
```

Example

Here is an example of the output from `diagnose debug sysinfo`:

```

=== file system information ===
Filesystem 1K-blocks Used Available Use% Mounted on
none 1471952 0 1471952 0% /dev/shm
none 65536 24 65512 0% /tmp
/dev/sda1 516040 75360 440680 15% /data
/dev/mdvg/mdlv 82561712 47014896 35546816 57% /var
/dev/mdvg/mdlv 82561712 47014896 35546816 57% /drive0
/dev/mdvg/mdlv 82561712 47014896 35546816 57% /Storage
/dev/loop0 9911 1122 8277 12% /var/dm/tcl-root

=== /tmp system information ===
drwxrwxrwx 2 root root 40 Sep 30 09:24 FortiManagerWS
srwxrwxrwx 1 root root 0 Sep 30 09:23 alertrd.req
srw-rw-rw- 1 root root 0 Sep 30 09:23 alertmail.sock
srw-rw-rw- 1 root root 0 Sep 30 09:23 alertmail_workflow.sock
-rw-rw-rw- 1 root root 4 Sep 30 09:22 cmdb_lock
srwxrwxrwx 1 root root 0 Sep 30 09:22 cmdbsocket
-rw-r--r-- 1 root root 52 Sep 30 09:23 crontab
-rw-r--r-- 1 root root 0 Sep 30 09:23 crontab.lock
srw-rw-rw- 1 root root 0 Sep 30 09:24 ddmclt.sock
-rw-rw-rw- 1 root root 4 Sep 30 09:24 django.pid
srw-rw-rw- 1 root root 0 Sep 30 09:23 dmserver.sock
-rw-rw-rw- 1 root root 0 Sep 30 09:22 dvm_sync_init
-rw-rw-rw- 1 root root 8 Sep 30 09:23 dvm_timestamp
drwx----- 2 root root 40 Sep 30 09:23 dynamic
srwxrwxrwx 1 root root 0 Sep 30 09:23 faz_svc
srwxrwxrwx 1 root root 0 Sep 30 09:24 fcgi.sock
srwxrwxrwx 1 root root 0 Sep 30 09:23 fmgd.domain
srwxrwxrwx 1 root root 0 Sep 30 09:24 httpcli.msg
srw-rw-rw- 1 root root 0 Sep 30 09:24 hwmnd.req
srwxrwxrwx 1 root root 0 Sep 30 09:23 log_stat.svr
srwxrwxrwx 1 root root 0 Sep 30 09:23 reliable_logging_path
srwxrwxrwx 1 root root 0 Sep 30 09:23 sql_plugin
srwxrwxrwx 1 root root 0 Sep 30 09:23 sql_report
-----wx--- 1 root root 0 Sep 30 09:37 sqlrpt.lck
srw-rw-rw- 1 root root 0 Sep 30 09:24 srchd.sock
srwxrwxrwx 1 root root 0 Sep 30 09:42 upm_forticlient.sock

=== resource use information ===
Program uses most memory: [gui control], pid 491, size 203m
Program uses most cpu: [/bin/cmdbsvr], pid 220, percent 0%

=== db locks information ===

```

debug sysinfo-log

Use this command to generate one system log information log file every two minutes.

Syntax

```
diagnose debug sysinfo-log {on | off}
```

debug sysinfo-log-backup

Use this command to backup all system information log files to an FTP server.

Syntax

```
diagnose debug sysinfo-log-backup <ip> <string> <username> <password>
```

Variable	Description
<ip>	Enter the FTP server IP address.
<string>	Enter the path or filename to save to the FTP server.
<username>	Enter the user name for the FTP server.
<password>	Enter the password for the FTP server.

debug sysinfo-log-list

Use this command to show system information elogs.

Syntax

```
diagnose debug sysinfo-log-list <integer>
```

Variable	Description
<integer>	Display the last n elogs. Default: 10

debug timestamp

Use this command to enable or disable debug timestamp.

Syntax

```
diagnose debug timestamp {enable | disable}
```

debug vminfo

Use this command to show VM license information.

Syntax

```
diagnose debug vminfo
```



This command is only available on FortiManager VM models.

Example

Here is an example of the output from `diagnose debug vminfo`:

```
ValidLicense Type: 5000UG
Table size:
Maximum dev: 6120
```

dlp-archives

Use this command to manage the DLP archives.

Syntax

```
diagnose dlp-archives quar-cache list-all-process
diagnose dlp-archives quar-cache kill-process <pid>
diagnose dlp-archives rebuild-quar-db
diagnose dlp-archives statistics {show | flush}
diagnose dlp-archives status
```

Variable	Description
quar-cache list-all-process	List all processes that are using the quarantine cache.
quar-cache kill-process <pid>	Kill a process that is using the quarantine cache.
rebuild-quar-db	Rebuild Quarantine Cache DB
statistics {show flush}	Display or flush the quarantined and DLP archived file statistics. Select one of the following: <ul style="list-style-type: none"><code>flush</code>: Flush quarantined and DLP archived file statistics.<code>show</code>: Display quarantined and DLP archived file statistics.
status	Running status.

dvm

Use the following commands for DVM related settings:

dvm adom

Use this command to list ADOMs.

Syntax

```
diagnose dvm adom list
```

Variable	Description
list	List ADOMs, state, product, OS version (OSVER), major release (MR), name, mode, and VPN management.

dvm capability

Use this command to set the DVM capability.

Syntax

```
diagnose dvm capability set {all | standard}
diagnose dvm capability show
```

Variable	Description
set {all standard}	Set the capability to all or standard.
show	Show what the capability is set to.

dvm chassis

Use this command to list chassis.

Syntax

```
diagnose dvm chassis list
```

Variable	Description
list	List chassis.

dvm check-integrity

Use this command to check the DVM database integrity.

Syntax

```
diagnose dvm check-integrity
```

Example

Here is an example of the output from `diagnose dvm check-integrity`:

```
[1/11] Checking object memberships ... correct
[2/11] Checking device nodes ... correct
[3/11] Checking device vdoms ... correct
[4/11] Checking device ADOM memberships ... correct
[5/11] Checking devices being deleted ... correct
[6/11] Checking devices not supported ... correct
[7/11] Checking devices state ... correct
[8/11] Checking groups ... correct
[9/11] Checking group membership ... correct
[10/11] Checking device locks ... correct
[11/11] Checking task database ... correct
```

dvm debug

Use this command to enable or disable debug channels.

Syntax

```
diagnose dvm debug {enable | disable} <channel> <channel> ... <channel>
```

dvm device

Use this command to list devices or objects referencing a device.

Syntax

```
diagnose dvm device dynobj <device>
diagnose dvm device list <device> <vdom>
diagnose dvm device delete <adom> <device>
```

Variable	Description
dynobj <device>	List dynamic objects on this device.
list <device> <vdom>	List devices. Optionally, enter a device or VDOM name.
delete <adom> <device>	Delete devices.

Example

Here is an example of the output from `diagnose dvm device dynobj <device>`:

```
=== VDOM root ===
Dynamic interface
Dynamic firewall address
  name: SSLVPN_TUNNEL_ADDR1
  name: all
Dynamic firewall address6
Dynamic firewall vip
Dynamic firewall vip6
Dynamic firewall vip46
Dynamic firewall vip64
Dynamic firewall ippool
Dynamic firewall ippool6
Dynamic certificate local
Dynamic vpn tunnel
```

dvm device-tree-update

Use this command to enable or disable device tree automatic updates.

Syntax

```
diagnose dvm device-tree-update {enable | disable}
```

dvm extender

Use these commands to list FortiExtender devices and synchronize data by JSON.

Syntax

```
diagnose dvm extender list
diagnose dvm extender sync-extender-data <device>
```

```
diagnose dvm extender get-extender-modem-ip <device> <id>
```

Variable	Description
list	List FortiExtender devices.
sync-extender-data	Synchronize FortiExtender data by JSON.
get-extender-modem-ip	Get the FortiExtender modem IP address by JSON.
<device>	Enter the device name.
<id>	Enter the FortiExtender ID.

dvm group

Use this command to list groups.

Syntax

```
diagnose dvm group list
```

dvm lock

Use this command to print the DVM lock states.

Syntax

```
diagnose dvm lock
```

Example

Here is an example of the output from `diagnose dvm lock`:

```
DVM lock state = unlocked
Global database pending read: unlocked
Global database pending write: unlocked
Global database reserved read: unlocked
Global database reserved write: unlocked
Global database shared read: unlocked
Global database shared write: unlocked
```

dvm proc

Use this command to list DVM processes.

Syntax

```
diagnose dvm proc list
```

Example

This example shows the output from `diagnose dvm proc list`:

```
dvmcmd group id=3632
dvmcmd process 3632 is running control
Process is healthy.
dvmcore is running normally.
```

dvm supported-platforms

Use this command to list supported platforms and firmware versions.

Syntax

```
diagnose dvm supported-platforms list detail
```

Variable	Description
list	List support platforms.
detail	Show detail with syntax support.

dvm task

Use this command to repair or reset the task database.

Syntax

```
diagnose dvm task list <adom> <type>
diagnose dvm task repair
diagnose dvm task reset
```

Variable	Description
list <adom> <type>	List task database information.
repair	Repair the task database while preserving existing data where possible. The FortiManager will reboot after the repairs.
reset	Reset the task database to its factory default state. All existing tasks and the task history will be erased. The FortiManager will reboot after the reset.

Example

This example shows the output for `diagnose dvm task root all`:

```
ADOM: root
ID Source Description User Status Start Time
-----
112 device_manager adddevtitle admin done Wed Jan 23 15:39:24 2013
113 device_manager deldevtitle admin done Wed Jan 23 15:51:10 2013
114 device_manager adddevtitle admin done Wed Jan 23 15:52:19 2013
115 import_dev_objs Import Device Objs/Policy admin done Wed Jan 23 15:52:55 2013
116 import_dev_objs Import Device Objs/Policy admin done Wed Jan 23 15:53:04 2013
117 import_dev_objs Import Device Objs/Policy admin done Wed Jan 23 15:53:08 2013
118 import_dev_objs Import Device Objs/Policy admin done Wed Jan 23 15:53:13 2013
132 device_manager adddeldevtitle admin done Thu Jan 24 17:55:17 2013
```

```

133 device_manager adddeldevtitle admin done Thu Jan 31 18:34:25 2013
134 device_manager adddeldevtitle admin done Mon Mar 25 16:26:35 2013
135 device_manager upddevtitle admin done Tue Mar 26 09:15:20 2013
136 device_manager deldevtitle admin done Tue Mar 26 09:16:48 2013
137 device_manager adddeldevtitle admin done Tue Mar 26 09:18:32 2013
138 device_manager deldevtitle admin done Tue Mar 26 09:22:49 2013
139 device_manager adddeldevtitle admin done Tue Mar 26 09:23:48 2013
140 device_manager deldevtitle admin done Tue Mar 26 09:30:20 2013
141 device_manager adddeldevtitle admin done Tue Mar 26 09:33:34 2013
142 device_manager deldevtitle admin done Tue Mar 26 09:35:06 2013
143 device_manager adddeldevtitle admin done Tue Mar 26 09:38:41 2013
144 device_manager adddeldevtitle admin done Tue Mar 26 09:59:18 2013
145 device_manager deldevtitle admin done Tue Mar 26 10:08:16 2013
146 device_manager deldevtitle admin done Tue Mar 26 10:08:26 2013
147 device_manager adddevtitle admin done Tue Mar 26 14:40:54 2013
148 import_dev_objs Import Device Objs/Policy admin done Tue Mar 26 14:42:05 2013

```

dvm transaction-flag

Use this command to edit or display DVM transaction flags.

Syntax

```
diagnose dvm transaction-flag {abort | debug | none}
```

fgfm

Use this command to get installation session, object, and session lists.

Syntax

```

diagnose fgfm install-session
diagnose fgfm object-list
diagnose fgfm session-list <device ID>

```

Variable	Description
install-session	Get installations session lists.
object-list	Get object lists.
session-list <device ID>	Get session lists.

fmnetwork

Use the following commands for network related settings.

fmnetwork arp

Use this command to manage ARP.

Syntax

```
diagnose fmnetwork arp del <intf-name> <IP>
diagnose fmnetwork arp list
```

Variable	Description
del <intf-name> <IP>	Delete an ARP entry.
list	List ARP entries.

Example

This example shows the output for `diagnose fmnetwork apr list`:

```
index=2 ifname=port1 10.2.115.20 00:09:0f:ed:bc:f3 state=00000002 use=2954 confirm=2954
update=2508 ref=3
index=1 ifname=lo 0.0.0.0 00:00:00:00:00:00 state=00000040 use=172515 confirm=835387
update=2096758 ref=2
index=2 ifname=port1 10.2.115.36 00:0c:29:ce:81:98 state=00000004 use=2978 confirm=2978
update=23 ref=2
index=2 ifname=port1 10.2.115.37 00:0c:29:8f:a2:8e state=00000002 use=2658 confirm=2658
update=2508 ref=3
index=2 ifname=port1 10.2.117.138 00:09:0f:77:05:28 state=00000002 use=2996
confirm=2996 update=2510 ref=3
index=2 ifname=port1 10.2.0.250 00:09:0f:48:91:b7 state=00000002 use=706 confirm=0
update=553 ref=19
index=2 ifname=port1 10.2.66.95 00:09:0f:09:00:00 state=00000002 use=2828 confirm=2828
update=2483 ref=3
index=2 ifname=port1 10.2.118.24 state=00000020 use=2701 confirm=2094709 update=2401
ref=2
```

fmnetwork interface

Use this command to view interface information.

Syntax

```
diagnose fmnetwork interface detail <portX>
diagnose fmnetwork interface list <portX>
```

Variable	Description
detail <portX>	View a specific interface's details.
list <portX>	List all interface details.

Example

Here is an example of the output from `diagnose fmnetwork interface list port1`:

```
port1 Link encap:Ethernet HWaddr D4:AE:52:86:F4:52
inet addr:10.2.60.101 Bcast:10.2.255.255 Mask:255.255.0.0
inet6 addr: fe80::d6ae:52ff:fe86:f452/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:26988508 errors:0 dropped:0 overruns:0 frame:0
TX packets:38322005 errors:0 dropped:0 overruns:0 carrier:0
```



```
collisions:0 txqueuelen:1000
RX bytes:4165017288 (3.8 GiB) TX bytes:54518196952 (50.7 GiB)
Interrupt:28 Memory:d6000000-d6012800
```

fmnetwork netstat

Use this command to view network statistics.

Syntax

```
diagnose fmnetwork netstat list [-r]
diagnose fmnetwork netstat tcp [-r]
diagnose fmnetwork netstat udp [-r]
```

Variable	Description
list [-r]	List all connections, or use -r to list only resolved IP addresses.
tcp [-r]	List all TCP connections, or use -r to list only resolved IP addresses.
udp [-r]	List all UDP connections, or use -r to list only resolved IP addresses.

Example

Here is an example of the output from `diagnose fmnetwork netstat tcp -r`:

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 FMG-VM:9090 *:* LISTEN
tcp 0 0 *:6020 *:* LISTEN
tcp 0 0 *:8900 *:* LISTEN
tcp 0 0 *:8901 *:* LISTEN
tcp 0 0 *:8080 *:* LISTEN
tcp 0 0 *:22 *:* LISTEN
tcp 0 0 *:telnet *:* LISTEN
tcp 0 0 *:8890 *:* LISTEN
tcp 0 0 *:8891 *:* LISTEN
tcp 0 0 *:541 *:* LISTEN
```

fmupdate

Use this command to diagnose update services.

Syntax

```
diagnose fmupdate add-device <serial> <ip> <firmware> <build>
diagnose fmupdate deldevice {fct | fds | fgd | fgc} <serialnum> <uid>
diagnose fmupdate dellog
diagnose fmupdate fct-configure
diagnose fmupdate fct-dbcontract
diagnose fmupdate fct-delserverlist
diagnose fmupdate fct-getobject
diagnose fmupdate fct-serverlist
diagnose fmupdate fct-update-status
```

```

diagnose fmupdate fct-updatenow
diagnose fmupdate fds-configure
diagnose fmupdate fds-dbcontract
diagnose fmupdate fds-delservelist
diagnose fmupdate fds-dump-breg
diagnose fmupdate fds-dump-srul
diagnose fmupdate fds-get-downstream-device <serialnum>
diagnose fmupdate fds-getobject
diagnose fmupdate fds-serverlist
diagnose fmupdate fds-service-info
diagnose fmupdate fds-update-status
diagnose fmupdate fds-updatenow
diagnose fmupdate fgc-configure
diagnose fmupdate fgc-delservelist
diagnose fmupdate fgc-serverlist
diagnose fmupdate fgc-update-status
diagnose fmupdate fgd-bandwidth {1h | 6h | 12h | 24h | 7d | 30d}
diagnose fmupdate fgd-configure
diagnose fmupdate fgd-dbcontract
diagnose fmupdate fgd-dbver {wf | as | av-query}
diagnose fmupdate fgd-delservelist
diagnose fmupdate fgd-get-downstream-device
diagnose fmupdate fgd-serverlist
diagnose fmupdate fgd-service-info
diagnose fmupdate fgd-test-client <ip> <serialnum> <string>
diagnose fmupdate fgd-update-status
diagnose fmupdate fgd-updatenow
diagnose fmupdate fgd-url-rating <serialnum> <version> <url>
diagnose fmupdate fgd-wfas-clear-log
diagnose fmupdate fgd-wfas-log {name | ip} <string>
diagnose fmupdate fgd-wfas-rate {wf | av | as_ip | as_url | as_hash}
diagnose fmupdate fgd-wfdevice-stat {10m | 30m | 1h | 6h | 12h | 24h | 7d} <serialnum>
diagnose fmupdate fgd-wfserver-stat {top10sites | top10devices} {10m | 30m | 1h | 6h | 12h | 24h | 7d}
diagnose fmupdate fgt-del-statistics
diagnose fmupdate fgt-del-um-db
diagnose fmupdate fmg-statistic-info
diagnose fmupdate fortitoken {seriallist | add | del} {add | del | required}
diagnose fmupdate getdevice {fct | fds | fgd | fgc} <serialnum>
diagnose fmupdate service-restart {fds | fct | fgd | fgc}
diagnose fmupdate show-bandwidth {fct | fgt | fml | faz} <serialnum>
diagnose fmupdate show-dev-obj <serialnum>
diagnose fmupdate view-linkd-log {fct | fds | fgd | fgc}
diagnose fmupdate vm-license

```

Variable	Description
add-device <serial> <ip> <firmware> <build>	Add an unregistered device. The build number is optional.

Variable	Description
deldevice {fct fds fgd fgc} <serialnum> <uid>	Delete a device. The UID applies only to FortiClient devices.
dellog	Delete log for FDS and FortiGuard update events.
fct-configure	Dump the FortiClient running configuration.
fct-dbcontract	Dump the FortiClient subscriber contract.
fct-delservicelist	Dump the FortiClient server list file fdni.dat.
fct-getobject	Get the version of all FortiClient objects.
fct-servicelist	Dump the FortiClient server list.
fct-update-status	Display the FortiClient update status.
fct-updatenow	Update the FortiClient antivirus/IPS immediately.
fds-configure	Dump the FDS running configuration.
fds-dbcontract	Dump the FDS subscriber contract
fds-delservicelist	Delete the FDS server list file fdni.dat.
fds-dump-breg	Dump the FDS beta serial numbers.
fds-dump-srul	Dump the FDS select filtering rules.
fds-get-downstream-device <serialnum>	Get information of all downstream FortiGate antivirus-IPS devices. Optionally, enter the device serial number.
fds-getobject	Get the version of all FortiGate objects.
fds-servicelist	Dump the FDS server list.
fds-service-info	Display FDS service information.
fds-update-status	Display the FDS update status.
fds-updatenow	Update the FortiGate antivirus/IPS immediately.
fgc-configure	Dump the FGC running configuration.
fgc-delservicelist	Delete the FGC server list file fdni.dat.

Variable	Description
fgc-serverlist	Dump the FGC server list.
fgc-update-status	Display the FGC update status.
fgd-bandwidth {1h 6h 12h 24h 7d 30d}	Display the download bandwidth.
fgd-configure	Dump the FortiGuard running configuration.
fgd-dbcontract	Dump the FortiGuard subscriber contract.
fgd-dbver {wf as av- query}	Get the version of the database. Optionally, enter the database type.
fgd-delservice	Delete the FortiGuard service list file fdni.dat.
fgd-get-downstream-device	Get information on all downstream FortiGate web filter and spam devices.
fgd-serverlist	Dump the FortiGuard server list.
fgd-service-info	Display FortiGuard service information.
fgd-test-client <ip> <serialnum> <string>	Execute FortiGuard test client. Optionally, enter the hostname or IP address of the FGD server, the serial number of the device, and the query number per second or URL.
fgd-update-status	Display the Fortiguard update status.
fgd-updatenow	Update the FortiGate web filter / antispam immediately.
fgd-url-rating <serialnum> <version> <url>	Rate URLs within the FortiManager database using the FortiGate serial number. Optionally, enter the category version and URL.
fgd-wfas-clear-log	Clear the FortiGuard service log file.
fgd-wfas-log {name ip} <string>	View the FortiGuard service log file. Optionally, enter the device filter type, and device name or IP address.
fgd-wfas-rate {wf av as_ ip as_url as_hash}	Get the web filter / antispam rating speed. Optionally, enter the server type.

Variable	Description
fgd-wfdevice-stat {10m 30m 1h 6h 12h 24h 7d} <serialnum>	Display web filter device statistics. Optionally, enter a specific device's serial number.
fgd-wfserver-stat {top10sites top10devices} {10m 30m 1h 6h 12h 24h 7d}	Display web filter server statistics for the top 10 sites or devices. Optionally, enter the time apn to cover.
fgt-del-statistics	Remove all statistics (antivirus / IPS and web filter / antispam). This command requires a reboot.
fgt-del-um-db	Remove UM and UM-GUI databases. This command requires a reboot. Note: um.db is a sqlite3 database that update manager uses internally. It will store AV/IPS package information of downloaded packages. This command removed the database file information. The package is not removed. After the reboot, the database will be recreated. Use this command if you suspect the database file is corrupted.
fmg-statistic-info	Display statistic information for FortiManager and Java Client.
fortitoken {seriallist add del} {add del required}	FortiToken related operations.
getdevice {fct fds fgd fgc} <serialnum>	Get device information. Optionally, enter a serial number.
service-restart {fds fct fgd fgc}	Restart linkd service.
show-bandwidth {fct fgt fml faz} <serialnum>	Display download bandwidth. Optionally, enter a serial number.
show-dev-obj <serialnum>	Display an objects version of a device. Optionally, enter a serial number.
view-linkd-log {fct fds fgd fgc}	View the linkd log file.

Variable	Description
vm-license	Dump the FortiGate VM license.

Example

To view antispam server statistics for the past seven days, enter the following:

```
diagnose fmupdate fgd-asserver_stat 7d
```

The command returns information like this:

```
Server Statistics
Total Spam Look-ups: 47
Total # Spam: 21 (45%)
Total # Non-spam:26 (55%)
Estimated bandwidth usage:17MB
```

fortilogd

Use this command to view FortiLog daemon information.

Syntax

```
diagnose fortilogd msgrate
diagnose fortilogd msgrate-device
diagnose fortilogd msgrate-total
diagnose fortilogd msgrate-type
diagnose fortilogd msgstat <flush>
diagnose fortilogd lograte
diagnose fortilogd status
```

Variable	Description
msgrate	Display log message rate.
msgrate-device	Display log message rate devices.
msgrate-total	Display log message rate totals.
msgrate-type	Display log message rate types.
msgstat	Display log message status.
lograte	Display the log rate.
<flush>	Reset the log message status.
status	Running status.

Example

This example shows the output for `diagnose fortilogd status`:

```

fortilogd is starting
config socket OK
cmdb socket OK
cmdb register log.device OK
cmdb register log.settings OK
log socket OK
reliable log socket OK

```

fwmanager

Use this command to manage firmware.

Syntax

```

diagnose fwmanager cancel-devsched <string> <firmware_version> <release_type> <build_num>
<date_time>
diagnose fwmanager cancel-grpsched <string> <firmware_version> <release_type> <build_num>
<date_time>
diagnose fwmanager delete-all
diagnose fwmanager delete-imported-images
diagnose fwmanager delete-offical-images
diagnose fwmanager delete-serverlist
diagnose fwmanager fwm-log
diagnose fwmanager getall-schedule
diagnose fwmanager getdev-schedule <string>
diagnose fwmanager getgrp-schedule <string>
diagnose fwmanager imported-imagelist
diagnose fwmanager official-imagelist
diagnose fwmanager reset-schedule-database
diagnose fwmanager set-devsched <string> <firmware_version> <release_type> <build_num>
<date_time>
diagnose fwmanager set-grpsched <string> <firmware_version> <release_type> <build_num>
<date_time>

```

Variable	Description
cancel-devsched <string> <firmware_version> <release_type> <build_num> <date_time>	Cancel an upgrade schedule for a device. For special branches, the release type is the branch point. The build number for official releases is always – 1, for special releases it is the build number. The date and time format is: YYYY/MM/DD_hh:mm:ss
cancel-grpsched <string> <firmware_version> <release_type> <build_num> <date_time>	Cancel an upgrade schedule for a group. For special branches, the release type is the branch point. The build number for official releases is always – 1, for special releases it is the build number. The date and time format is: YYYY/MM/DD_hh:mm:ss

Variable	Description
delete-all	Remove everything in the firmware manager folder. This command requires a reboot.
delete-imported-images	Remove all imported images. This command requires a reboot.
delete-offical-images	Remove all official images. This command requires a reboot.
delete-serverlist	Remove the server list file (fdni.dat). This command requires a reboot.
fwm-log	View the firmware manager log file.
getall-schedule	Display all upgrade schedules recorded.
getdev-schedule <string>	Get scheduled upgrades for the device.
getgrp-schedule <string>	Get scheduled upgrades for this group.
imported-imagelist	Get the imported firmware image list
official-imagelist	Get the official firmware image list.
reset-schedule-database	Cleanup and initialize the schedule database and restart the server.
set-devsched <string> <firmware_version> <release_type> <build_num> <date_time>	Create an upgrade schedule for a device.
set-grpsched <string> <firmware_version> <release_type> <build_num> <date_time>	Create an upgrade schedule for a group.

ha

Use this command to manage high availability.

Syntax

```
diagnose ha debug-sync {on | off}  
diagnose ha dump-datalog  
diagnose ha force-resync  
diagnose ha stats
```

Variable	Description
debug-sync {on off}	Turn on synchronized data debug.
dump-datalog	Dump the HA data log.
force-resync	Force re-synchronization.
stats	Get HA statistics.

Example

To turn on debug synchronization, enter the following:

```
diagnose ha debug-sync on
```

hardware

Use this command to view hardware information.

Syntax

```
diagnose hardware info
```

Example

This example shows the output for `diagnose hardware info`:

```
### CPU info  
processor : 0  
vendor_id : GenuineIntel  
cpu family : 6  
model : 45  
model name : Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz  
stepping : 7  
cpu MHz : 1899.992  
cache size : 15360 KB  
fpu : yes  
fpu_exception : yes  
cpuid level : 13  
wp : yes  
flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush  
mmx fxsr sse sse2 ss syscall nx lm constant_tsc up rep_good pni pclmulqdq ssse3  
cx16 sse4_1 sse4_2 popcnt aes xsave avx hypervisor lahf_lm xsaveopt  
bogomips : 3799.98  
clflush size : 64  
cache_alignment : 64
```

address sizes : 42 bits physical, 48 bits virtual

power management:

Memory info

MemTotal: 2060172 kB

MemFree: 359316 kB

Buffers: 140056 kB

Cached: 668136 kB

SwapCached: 0 kB

Active: 1034340 kB

Inactive: 431328 kB

Active(anon): 693372 kB

Inactive(anon): 17144 kB

Active(file): 340968 kB

Inactive(file): 414184 kB

Unevictable: 76660 kB

Mlocked: 76136 kB

SwapTotal: 2076536 kB

SwapFree: 2076536 kB

Dirty: 72 kB

Writeback: 0 kB

AnonPages: 734132 kB

Mapped: 79244 kB

Shmem: 39060 kB

Slab: 101752 kB

SReclaimable: 87052 kB

SUnreclaim: 14700 kB

KernelStack: 1928 kB

PageTables: 30772 kB

NFS_Unstable: 0 kB

Bounce: 0 kB

WritebackTmp: 0 kB

CommitLimit: 3106620 kB

Committed_AS: 6981052 kB

VmallocTotal: 34359738367 kB

VmallocUsed: 2736 kB

VmallocChunk: 34359727840 kB

DirectMap4k: 4032 kB

DirectMap2M: 2093056 kB

Disk info

major minor #blocks name

7 0 10240 loop0

3 0 2099200 hda

3 64 41943040 hdb

22 64 41943040 hdd

8 16 41943040 sdb

8 0 2099200 sda

8 1 524288 sdal

8 32 41943040 sdc

253 0 83877888 dm-0

RAID info

N/A

System time

local time: Tue Oct 21 14:54:43 2014

UTC time: Tue Oct 21 21:54:43 2014

log

Use this commands to view and manage device logging.

log device

Use this command to manage device logging.

Syntax

```
diagnose log device
```

Example

This example shows the output for diagnose log device:

```
Device Name Device ID Used Space(logs/database/quar/content/IPS) Allocated Space % Used
FK3K8A3407600133 FK3K8A3407600133 OMB(0 / 0 / 0 / 0 / 0 ) 1000MB 0.00%
FOC-32bit FGVM01EW12000001 OMB(0 / 0 / 0 / 0 / 0 ) 1000MB 0.00%
b147-37 FGVM02EW12000001 OMB(0 / 0 / 0 / 0 / 0 ) 1000MB 0.00%
FWF-60CM-Gen4 FW60CM3G11004076 OMB(0 / 0 / 0 / 0 / 0 ) 1000MB 0.00%
FG200B3911601438 FG200B3911601438 OMB(0 / 0 / 0 / 0 / 0 ) 1000MB 0.00%
FortiGate-VM64 FGVM04QX10091530 OMB(0 / 0 / 0 / 0 / 0 ) 1000MB 0.00%
FW60CM3G10003021 FW60CM3G10003021 OMB(0 / 0 / 0 / 0 / 0 ) 1000MB 0.00%
m-fwf60cm FW60CM1738042MDL OMB(0 / 0 / 0 / 0 / 0 ) 1000MB 0.00%
FW60CM3G11000082 FW60CM3G11000082 OMB(0 / 0 / 0 / 0 / 0 ) 1000MB 0.00%
fgtha-m-95 FGHA002041334518_CID OMB(0 / 0 / 0 / 0 / 0 ) 1000MB 0.00%
```

pm2

Use this command to print from and check the integrity of the policy manager database.

Syntax

```
diagnose pm2 check-integrity {all adom device global ips}
diagnose pm2 print <log-type>
```

Variable	Description
check-integrity {all adom device global ips}	Check policy manager database integrity. Multiple database categories can be checked at once.
print <log-type>	Print policy manager database log messages.

report

Use these commands to check the SQL database.

Syntax

```
diagnose report clean
diagnose report status {pending | running}
```

Variable	Description
clean	Cleanup the SQL report queue.
status {pending running}	Check status information on pending and running reports list.

sniffer

Use this command to perform a packet trace on one or more network interfaces.

Packet capture, also known as sniffing, records some or all of the packets seen by a network interface. By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiManager units have a built-in sniffer. Packet capture on FortiManager units is similar to that of FortiGate units. Packet capture is displayed on the CLI, which you may be able to save to a file for later analysis, depending on your CLI client.

Packet capture output is printed to your CLI display until you stop it by pressing Control + C, or until it reaches the number of packets that you have specified to capture.



Packet capture can be very resource intensive. To minimize the performance impact on your FortiManager unit, use packet capture only during periods of minimal traffic, with a serial console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

Syntax

```
diagnose sniffer packet <interface_name> <filter_str> <verbose> <count>
```

Variable	Description
<interface_name>	Type the name of a network interface whose packets you want to capture, such as <code>port1</code> , or type <code>any</code> to capture packets on all network interfaces.

Variable	Description
<filter_str>	<p>Type either <code>none</code> to capture all packets, or type a filter that specifies which protocols and port numbers that you do or do not want to capture, such as <code>'tcp port 25'</code>. Surround the filter string in quotes.</p> <p>The filter uses the following syntax:</p> <pre>'[[src dst] host {<host1_fqdn> <host1_ipv4>}] [and or] [[src dst] host {<host2_fqdn> <host2_ipv4>}] [and or] [[arp ip gre esp udp tcp] port <port1_int>] [and or] [[arp ip gre esp udp tcp] port <port2_int>]'</pre> <p>To display only the traffic between two hosts, specify the IP addresses of both hosts. To display only forward or only reply packets, indicate which host is the source, and which is the destination.</p> <p>For example, to display UDP port 1812 traffic between 1.example.com and either 2.example.com or 3.example.com, you would enter:</p> <pre>'udp and port 1812 and src host 1.example.com and dst \(2.example.com or 2.example.com \)'</pre>
<verbose>	<p>Type one of the following numbers indicating the depth of packet headers and payloads to capture:</p> <ul style="list-style-type: none"> • 1: header only • 2: IP header and payload • 3: Ethernet header and payload <p>For troubleshooting purposes, Fortinet Technical Support may request the most verbose level (3). Default: 1</p>
<count>	<p>Type the number of packets to capture before stopping. If you do not specify a number, the command will continue to capture packets until you press <code>Control + C</code>.</p>

Example 1

The following example captures the first three packets' worth of traffic, of any port number or protocol and between any source and destination (a filter of `none`), that passes through the network interface named `port1`. The capture uses a low level of verbosity (indicated by 1).

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiManager# diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.918957 192.168.0.1.36701 -> 192.168.0.2.22: ack 2598697710
0.919024 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697710 ack 2587945850
0.919061 192.168.0.2.22 -> 192.168.0.1.36701: psh 2598697826 ack 2587945850
```

If you are familiar with the TCP protocol, you may notice that the packets are from the middle of a TCP connection. Because port 22 is used (highlighted above in bold), which is the standard port number for SSH, the packets might be from an SSH session.

Example 2

The following example captures packets traffic on TCP port 80 (typically HTTP) between two hosts, 192.168.0.1 and 192.168.0.2. The capture uses a low level of verbosity (indicated by 1). Because the filter does not specify

either host as the source or destination in the IP header (`src` or `dst`), the sniffer captures both forward and reply traffic.

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Control + C. The sniffer then confirms that five packets were seen by that network interface.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiManager# diag sniffer packet port1 'host 192.168.0.2 or host 192.168.0.1 and tcp port 80' 1
192.168.0.2.3625 -> 192.168.0.1.80: syn 2057246590
192.168.0.1.80 -> 192.168.0.2.3625: syn 3291168205 ack 2057246591
192.168.0.2.3625 -> 192.168.0.1.80: ack 3291168206
192.168.0.2.3625 -> 192.168.0.1.80: psh 2057246591 ack 3291168206
192.168.0.1.80 -> 192.168.0.2.3625: ack 2057247265
5 packets received by filter
0 packets dropped by kernel
```

Example 3

The following example captures all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP address. The capture uses a high level of verbosity (indicated by 3).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Control + C. The sniffer then confirms that five packets were seen by that network interface.

Verbose output can be very long. As a result, output shown below is truncated after only one packet.

Commands that you would type are highlighted in bold; responses from the Fortinet unit are not in bold.

```
FortiManager # diag sniffer port1 'tcp port 443' 3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000 0009 0f09 0001 0009 0f89 2914 0800 4500 .....E.
0x0010 003c 73d1 4000 4006 3bc6 d157 fede ac16 .<s.@.@.;..W....
0x0020 0ed8 c442 01bb 2d66 d8d2 0000 0000 a002 ...B..-f.....
0x0030 16d0 4f72 0000 0204 05b4 0402 080a 03ab ..Or.....
0x0040 86bb 0000 0000 0103 0303 .....
```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encoding other than US-ASCII. It is usually preferable to analyze the output by loading it into a network protocol analyzer application such as Wireshark (<http://www.wireshark.org/>).

For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output. Methods may vary. See the documentation for your CLI client.

Requirements

- terminal emulation software such as [PuTTY](#)
- a plain text editor such as Notepad
- a [Perl](#) interpreter
- network protocol analyzer software such as [Wireshark](#)

To view packet capture output using PuTTY and Wireshark:

1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the Fortinet appliance using either a local serial console, SSH, or Telnet connection.
3. Type the packet capture command, such as:

```
diag sniffer packet port1 'tcp port 541' 3 100
```

 but do not press Enter yet.
4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select *Change Settings*.
 A dialog appears where you can configure PuTTY to save output to a plain text file.
5. In the *Category* tree on the left, go to *Session > Logging*.
6. In *Session logging*, select *Printable output*.
7. In *Log file name*, click the *Browse* button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file. You do not need to save it with the `.log` file extension.
8. Click *Apply*.
9. Press *Enter* to send the CLI command to the unit, beginning packet capture.
10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press `Control + C` to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad.
13. Delete the first and last lines, which look like this:

```
===== PuTTY log 7/14/2016.07.25 11:34:40 =====  
Fortinet-2000 #
```

 These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.
14. Convert the plain text file to a format recognizable by your network protocol analyzer application.
 You can convert the plain text file to a format (`.pcap`) recognizable by Wireshark (formerly called Ethereal) using the `fgt2eth.pl` Perl script. To download `fgt2eth.pl`, see the Fortinet Knowledge Base article [Using the FortiOS built-in packet sniffer](#).



The `fgt2eth.pl` script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

To use `fgt2eth.pl`, open a command prompt, then enter a command such as the following:

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
- `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
- `packet_capture.pcap` is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved

15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

For additional information on packet capture, see the Fortinet Knowledge Base article [Using the FortiOS built-in packet sniffer](#).

sql

Use these commands to diagnose the SQL database.

Syntax

```
diagnose sql config debug-filter [{set | test} <string>]
diagnose sql config deferred-index-timespan [set <value>]
diagnose sql config top-dev set [{log-thres | num-max}] <integer>
diagnose sql gui-rpt-shm {list-all | clear} <num>
diagnose sql process list [full]
diagnose sql process kill <pid>
diagnose sql rebuild-report-hcache <start-time> <end-time>
diagnose sql remove hcache <device-id>
diagnose sql remove query-cache
diagnose sql remove tmp-table
diagnose sql show <db-size | hcache-size | log-stfile>
diagnose sql show log-filters
diagnose sql status rebuild-db
diagnose sql status run_sql_rpt
diagnose sql status sql_hcache_chk
diagnose sql status sqlplugind
diagnose sql status sqlreportd
diagnose sql upload <host> <directory> <username> <password>
```

Variable	Description
config debug-filter [{set test} <string>]	Set or test the sqlplugin debug filter.
config deferred-index-timespan [set <value>]	Set the timespan for the deferred index.
config top-dev set [{log-thres num-max}] <integer>	Set the SQL plugin top devices settings including: <ul style="list-style-type: none"> log-thres: Log threshold of top devices. num-max: Maximum number of top devices. Select a number between 0 and 1000.
gui-rpt-shm {list-all clear} <num>	List or clear all asynchronous GUI report shared memory slot information.

Variable	Description
<code>process list [full]</code>	List running query processes.
<code>process kill <pid></code>	Kill a running query.
<code>rebuild-report-hcache <start-time> <end-time></code>	Rebuild <code>hcache</code> for report. Enter the start time/end time in the format "yyyy-mm-dd hh:mm:ss".
<code>remove hcache <device-id></code>	Remove <code>hcache</code> .
<code>remove query-cache</code>	Remove SQL query cache for log search.
<code>remove tmp-table</code>	Remove temporary tables.
<code>show <db-size hcache-size log-stfile></code>	Show the database or <code>hcache</code> size and <code>logstatus</code> file.
<code>show log-filters</code>	Show log view searching filters.
<code>status rebuild-db</code>	Show the SQL log database rebuild status.
<code>status run_sql_rpt</code>	Show the <code>run_sql_rpt</code> status.
<code>status sql_hcache_chk</code>	Show the report <code>hcache</code> status.
<code>status sqlplugind</code>	Show the <code>sqlplugind</code> daemon status.
<code>status sqlreportd</code>	Show the <code>sqlreportd</code> daemon status.
<code>upload <host> <directory> <username> <password></code>	Upload <code>sqlplugind</code> messages or <code>pgsvr</code> logs via FTP.

system

Use the following commands for system related settings.

system admin-session

Use this command to view login session information.

Syntax

```
diagnose system admin-session kill <sid>
diagnose system admin-session list
diagnose system admin-session status
```

Variable	Description
kill <sid>	Kill a current session.
list	List login sessions.
status	Show the current session.

Example

Here is an example of the output from `diagnose system admin-session status`:

```
session_id: 31521 (seq: 4)
username: admin
admin template: admin
from: jsconsole(10.2.0.250)
profile: Super_User (type 3)
adom: root
session length: 198 (seconds)
```

system disk

Use this command to view disk diagnostic information.

Syntax

```
diagnose system disk attributes
diagnose system disk disable
diagnose system disk enable
diagnose system disk health
diagnose system disk info
diagnose system disk errors
```

Variable	Description
attributes	Show vendor specific SMART attributes.
disable	Disable SMART support.
enable	Enable SMART support.
health	Show the SMART health status.

Variable	Description
info	Show the SMART information.
errors	Show the SMART error logs.

Example

This is an example of the output from `diagnose system disk health`:

```
Disk 1: SMART overall-health self-assessment test result: PASSED
Disk 2: SMART overall-health self-assessment test result: PASSED
Disk 3: SMART overall-health self-assessment test result: PASSED
Disk 4: SMART overall-health self-assessment test result: PASSED
```

system export

Use this command to export logs.

Syntax

```
diagnose system export crashlog <ftp server> <user> <password> [remote path] [filename]
diagnose system export dminstallog <devid> <server> <user> <password> [remote path]
[filename]
diagnose system export fmwslog <sftp | ftp> <type> <ftp server> <username> <password>
<directory> <filename>
diagnose system export umlog {ftp | sftp} <type> <server> <user> <password> [remote path]
[filename]
diagnose system export upgradelog <ftp server>
```

Variable	Description
crashlog <ftp server> <user> <password> [remote path] [filename]	Export the crash log.
dminstallog <devid> <server> <user> <password> [remote path] [filename]	Export deployment manager install log.
fmwslog <sftp ftp> <type> <ftp server> <username> <password> <directory> <filename>	Export web service log files.

Variable	Description
umlog {ftp sftp} <type> <server> <user> <password> [remote path] [filename]	Export the update manager and firmware manager log files. The type options are: fdslinkd, fctlinkd, fgdlinkd, usvr, update, service, misc, umad, and fwmlinkd
upgradelog <ftp server>	Export the upgrade error log.

system flash

Use this command to diagnose the flash memory.

Syntax

```
diagnose system flash list
```

Example

Here is an example of the output from `diagnose system flash list`:

```

ImageName Version TotalSize(KB) Used(KB) Use% BootImage RunningImage
primary FM-3KC-4.01-FW-build8308-200212 63461 29699 47% No No
secondary FM-3KC-5.00-FW-build0254-131025 63461 41812 66% Yes Yes

```

system fsck

Use this command to check and repair the filesystem.

Syntax

```
diagnose system fsck harddisk
```

Variable	Description
harddisk	Check and repair the file system, then reboot the system.

system geoip

Use these commands to obtain geoip information. FortiManager uses a [MaxMind GeoLite](#) database of mappings between geographic regions and all public IP addresses that are known to originate from them.

Syntax

```

diagnose system geoip dump
diagnose system geoip info
diagnose system geoip ip

```

Example

This example shows the output for `diagnose system geoip info`:

```
Version: 1.019
Date: Fri Oct 4 16:56:02 2013
Copyright: Copyright (c) 2011 MaxMind Inc. All Rights Reserved.
```

This example shows the output for `diagnose system geoip ip 223.255.254.0`:

```
223.255.254.0 : SG - Singapore
```

system ntp

Use this command to list NTP server information.

Syntax

```
diagnose system ntp status
```

Example

This example shows the output for `diagnose system ntp status`:

```
server ntp1.fortinet.net (208.91.112.50) -- Clock is synchronized
server-version=4, stratum=11
reference time is d5049d6a.4c80f64e -- UTC Mon Apr 1 23:57:30 2013
clock offset is 0.052517 msec, root delay is 0 msec
root dispersion is 752 msec, peer dispersion is 4 msec
```

system print

Use this command to print server information.

Syntax

```
diagnose system print certificate
diagnose system print cpuinfo
diagnose system print df
diagnose system print hosts
diagnose system print interface <interface>
diagnose system print loadavg
diagnose system print netstat
diagnose system print partitions
diagnose system print route
diagnose system print rtcache
diagnose system print slabinfo
diagnose system print sockets
diagnose system print uptime
```

Variable	Description
certificate	Print the IPsec certificate.
cpuinfo	Print the CPU information.
df	Print the file system disk space usage.

Variable	Description
hosts	Print the static table lookup for host names.
interface <interface>	Print the information of the interface
loadavg	Print the average load of the system.
netstat	Print the network statistics.
partitions	Print the partition information of the system.
route	Print the main route list.
rtcache	Print the contents of the routing cache.
slabinfo	Print the slab allocator statistics.
sockets	Print the currently used socket ports.
uptime	Print how long the system has been running.

Example

Here is an example of the output from `diagnose system print df`:

```
Filesystem 1K-blocks Used Available Use% Mounted on
none 65536 0 65536 0% /dev/shm
none 65536 20 65516 1% /tmp
/dev/sda1 47595 28965 16173 65% /data
/dev/sdb3 9803784 723128 8582652 8% /var
/dev/sdb2 61927420 224212 58557480 1% /var/static
/dev/sdb4 9803784 132164 9173616 2% /var/misc
/dev/sdb4 9803784 132164 9173616 2% /drive0
/dev/sdb4 9803784 132164 9173616 2% /Storage
/dev/loop0 9911 1043 8356 12% /var/dm/tcl-root
```

system process

Use this command to view and kill processes.

Syntax

```
diagnose system process kill <signal> <pid>
diagnose system process killall <module>
diagnose system process list
```

Variable	Description
kill <signal> <pid>	Kill a process.

Variable	Description
killall <module>	Kill all the related processes.
list	List all processes.

system raid

Use this command to view RAID information.

Syntax

```
diagnose system raid alarms
diagnose system raid hwinfo
diagnose system raid status
```

Variable	Description
alarms	Show RAID alarm logs.
hwinfo	Show RAID controller hardware information.
status	Show RAID status. This command displays the following information: RAID level, RAID status, RAID size, and hard disk information.

Example

Here is an example of the output from `diagnose system raid status`:

```
RAID Level: Raid-1
RAID Status: OK
RAID Size: 1953GB
Disk 1: OK Used 1953GB
Disk 2: Unavailable Not-Used 0GB
Disk 3: Unavailable Not-Used 0GB
Disk 4: Unavailable Not-Used 0GB
```

system route

Use this command to diagnose routes.

Syntax

```
diagnose system route list
```

Example

Here is an example of the output from `diagnose system route list`:

```
Destination Gateway Genmask Flags Metric Ref Use Iface
10.2.0.0 0.0.0.0 255.255.0.0 U 0 0 0 port1
169.254.0.0 0.0.0.0 255.255.0.0 U 0 0 0 svr_fgfm
169.254.0.0 0.0.0.0 255.255.0.0 U 0 0 0 svr_fgfm
0.0.0.0 10.2.115.20 0.0.0.0 UG 1 0 0 port1
```

system route6

Use this command to diagnose IPv6 routes.

Syntax

```
diagnose system route6 list
```

Example

Here is an example of the output from `diagnose system route list`:

```
Destination Gateway Intf Metric Priority
fe80::/64 :: port1 131080 256
fe80::/64 :: port2 131080 256
fe80::/64 :: port3 131080 256
fe80::/64 :: port4 131080 256
```

system server

Use this command to start the FortiManager server.

Syntax

```
diagnose system server start
```

test

Use the following commands to test the FortiManager.

test application

Use this command to test applications. Leave the integer value blank to see the available options for each command.

Syntax

```
diagnose test application fazcfgd <integer>
diagnose test application fazsvcg <integer>
diagnose test application fortilogd <integer>
diagnose test application logfiled <integer>
diagnose test application oftpd <integer>
diagnose test application snmpd <integer>
diagnose test application sqllogd <integer>
diagnose test application sqlrptcached <integer>
diagnose test application fazautormd <integer>
```

Variable	Description
fazcfgd <integer>	Test the FortiAnalyzer config daemon.

Variable	Description
fazsvcg <integer>	Test the FortiAnalyzer service daemon.
fortilogd <integer>	Test the FortiAnalyzer <code>fortilogd</code> daemon.
logfiled <integer>	Test the FortiAnalyzer log file daemon.
oftpd <integer>	Test the FortiAnalyzer <code>oftpd</code> daemon.
snmpd <integer>	Test the SNMP daemon.
sqllogd <integer>	Test the FortiAnalyzer <code>sqllog</code> daemon.
sqlrptcached <integer>	Test the FortiAnalyzer <code>sqlrptcache</code> daemon.
fazautormd <integer>	Test the FortiAnalyzer <code>autodelete</code> daemon.

test connection

Use this command to test connections.

Syntax

```
diagnose test connection mailserver <server-name> <account>
diagnose test connection syslogserver <server-name>
```

Variable	Description
mailserver <server-name> <account>	Test the connection to the mail server.
syslogserver <server-name>	Test the connection to the syslog server.

test deploymanager

Use this command to test the deployment manager.

Syntax

```
diagnose test deploymanager getcheckin <devid>
diagnose test deploymanager reloadconf <devid>
```

Variable	Description
getcheckin <devic>	Get configuration check-in information from the FortiGate.
reloadconf <devic>	Reload configuration from the FortiGate.

test policy-check

Use this command to test applications.

Syntax

```
diagnose test policy-check flush
diagnose test policy-check list
```

Variable	Description
flush	Flush all policy check sessions.
list	List all policy check sessions.

test search

Use this command to test the search daemon.

Syntax

```
diagnose test search flush
diagnose test search list
```

Variable	Description
flush	Flush all search sessions.
list	List all search sessions.

test sftp

Use this command to test the secure file transfer protocol (SFTP).

Syntax

```
diagnose test sftp auth <sftp server> <username> <password> <directory>
```

Variable	Description
auth <sftp server> <username> <password> <directory>	Test the scheduled backup. The directory variable represents the directory on the SFTP server where you want to put the file. The default directory is "/".

upload

Use these commands to perform request related actions.

upload clear

Use this command to clear the upload request.

Syntax

```
diagnose upload clear all
diagnose upload clear failed
```

Variable	Description
all	Clear all upload requests.
failed	Clear the failed upload requests.

upload force-retry

Use this command to retry the last failed upload request.

Syntax

```
diagnose upload force-entry
```

Example

Here is an example of the output from `diagnose upload force-retry`:

```
Force retry command has been issued.
```

upload status

Use this command to get the running status.

Syntax

```
diagnose upload status
```

vpn

Use this command to flush SAD entries and list tunnel information.

Syntax

```
diagnose vpn tunnel flush-SAD
diagnose vpn tunnel list
```

Variable	Description
<code>flush-SAD</code>	Flush the SAD entries.
<code>list</code>	List tunnel information.

get

The `get` command displays all settings, even if they are still in their default state.



Although not explicitly shown in this section, for all `config` commands, there are related `get` and `show` commands that display that part of the configuration. Get and show commands use the same syntax as their related `config` command, unless otherwise specified.



CLI commands and variables are case sensitive.

Unlike the `show` command, `get` requires that the object or table whose settings you want to display are specified, unless the command is being used from within an object or table.

For example, at the root prompt, this command would be valid:

```
get system status
```

and this command would not:

```
get
```

fmupdate analyzer

Use this command to view forward virus report to FDS setting.

Syntax

```
get fmupdate analyzer virusreport
```

fmupdate av-ips

Use these commands to view AV/IPS update settings.

Syntax

```
get fmupdate av-ips advanced-log
get fmupdate av-ips fct server-override
get fmupdate av-ips fgt server-override
get fmupdate av-ips push-override
get fmupdate av-ips push-override-to-client
get fmupdate av-ips update-schedule
get fmupdate av-ips web-proxy
```

Example

This example shows the output for `get fmupdate av-ips web-proxy`:

```
ip : 0.0.0.0
mode : proxy
password : *
port : 80
status : disable
username : (null)
```

fmupdate custom-url-list

Use this command to view the custom URL database.

Syntax

```
get fmupdate custom-url-list
```

fmupdate device-version

Use this command to view device version objects.

Syntax

```
get fmupdate device-version
```

Example

This example shows the output for `get fmupdate device-version`:

```
faz : 4.0 5.0
fct : 5.0
fgt : 3.0 4.0 5.0
fml : 3.0 4.0
fsa : 1.0
fsw :
```

fmupdate disk-quota

Use this command to view the disk quota for the update manager.

Syntax

```
get fmupdate disk-quota
```

fmupdate fct-services

Use this command to view FortiClient update services configuration.

Syntax

```
get fmupdate fct-services
```

Example

This example shows the output for `get fmupdate fct-services`:

```
status : enable
port : 80
```

fmupdate fds-setting

Use this command to view FDS parameters.

Syntax

```
get fmupdate fds-setting
```

Example

This example shows the output for `get fmupdate fds-setting`:

```
fds-pull-interval : 10
max-av-ips-version : 20
```

fmupdate multilayer

Use this command to view multilayer mode configuration.

Syntax

```
get fmupdate multilayer
```

fmupdate publicnetwork

Use this command to view public network configuration.

Syntax

```
get fmupdate publicnetwork
```

fmupdate server-access-priorities

Use this command to view server access priorities.

Syntax

```
get fmupdate server-access-priorities
```

Example

This example shows the output for `get fmupdate server-access-priorities`:

```
access-public : disable
av-ips : disable
private-server:
web-spam : enable
```

fmupdate server-override-status

Use this command to view server override status configuration.

Syntax

```
get fmupdate server-override status
```

fmupdate service

Use this command to view update manager service configuration.

Syntax

```
get fmupdate service
```

Example

This example shows the output for `get fmupdate service`:

```
avips : disable
query-antispam : disable
query-antivirus : disable
query-filequery : disable
query-webfilter : disable
use-cert : BIOS
```

fmupdate support-pre-fgt43

Use this command to view support for pre-fgt43 configuration.

Syntax

```
get fmupdate support-pre-fgt43
```

fmupdate web-spam

Use these commands to view web spam configuration.

Syntax

```
get fmupdate web-spam fct server-override
get fmupdate web-spam fgd-log
get fmupdate web-spam fgd-setting
get fmupdate web-spam fgt server-override
get fmupdate web-spam poll-frequency
get fmupdate web-spam web-proxy
```

Example

This example shows the output for `get fmupdate web-spam web-proxy`:

```
ip : 0.0.0.0
mode : proxy
password : *
port : 80
status : disable
username : (null)
```

system admin

Use these commands to view admin configuration.

Syntax

```
get system admin group <group name>
get system admin ldap <server entry name>
get system admin profile <profile ID>
get system admin radius <server entry name>
get system admin setting
get system admin tacacs <server entry name>
get system admin user <username>
```

Example

This example shows the output for `get system admin setting`:

```
access-banner : disable
admin-https-redirect: enable
admin_server_cert : server.crt
allow_register : disable
auto-update : disable
banner-message : (null)
chassis-mgmt : enable
chassis-update-interval: 15
demo-mode : disable
device_sync_status : enable
http_port : 80
https_port : 443
idle_timeout : 480
install-ifpolicy-only: enable
mgmt-addr : (null)
mgmt-fqdn : (null)
offline_mode : disable
register_passwd : *
```

```
show-add-multiple : enable
show-adom-central-nat-policies: disable
show-adom-devman : enable
show-adom-dos-policies: disable
show-adom-dynamic-objects: enable
show-adom-icap-policies: disable
show-adom-implicit-policy: disable
show-adom-ipv6-settings: enable
show-adom-policy-consistency-button: disable
show-adom-rtmlog : disable
show-adom-sniffer-policies: disable
show-adom-taskmon-button: disable
show-adom-terminal-button: disable
show-adom-voip-policies: disable
show-adom-vpnman : enable
show-adom-web-portal: enable
show-device-import-export: enable
show-foc-settings : disable
show-fortimail-settings: disable
show-fsw-settings : disable
show-global-object-settings: enable
show-global-policy-settings: enable
show_automatic_script: disable
show_grouping_script: disable
show_schedule_script: disable
show_tcl_script : disable
unreg_dev_opt : add_allow_service
webadmin_language : auto_detect
```

system alert-console

Use this command to view alert console information.

Syntax

```
get system alert-console
```

system alert-event

Use this command to view alert event information.

Syntax

```
get system alert-event <alert name>
```

system alertemail

Use this command to view alert email configuration.

Syntax

```
get system alertemail
```

Example

This example shows the output for `get system alertemail`:

```
authentication : enable
fromaddress : (null)
fromname : (null)
smtppassword : *
smtpport : 25
smtpserver : (null)
smtpuser : (null)
```

system auto-delete

Use this command to view automatic deletion policies for logs, reports, archived and quarantined files.

Syntax

```
get system auto-delete
```

system backup

Use the following commands to view backups:

Syntax

```
get system backup all-settings
get system backup status
```

Example

This example shows the output for `get system backup status`:

```
All-Settings Backup
Last Backup: Tue Jan 15 16:55:35 2013
Next Backup: N/A
```

system certificate

Use these commands to view certificate configuration.

Syntax

```
get system certificate ca <certificate name>
get system certificate crl <crl name>
get system certificate local <certificate name>
get system certificate oftp <certificate name>
```

```
get system certificate ssh <certificate name>
```

system dm

Use this command to view device manager information on your device.

Syntax

```
get system dm
```

Example

This example shows the output for `get system dm`:

```
concurrent-install-limit: 60
concurrent-install-script-limit: 60
discover-timeout : 6
dpm-logsize : 10000
fgfm-sock-timeout : 360
fgfm_keepalive_itvl : 120
force-remote-diff : disable
max-revs : 100
nr-retry : 1
retry : enable
retry-intvl : 15
rollback-allow-reboot: disable
script-logsize : 100
verify-install : enable
```

system dns

Use this command to view DNS configuration.

Syntax

```
get system dns
```

system fips

Use this command to view FIPS configuration.

Syntax

```
get system fips
```

system global

Use this command to view global configuration.

Syntax

```
get system global
```

Example

This example shows the output for `get system global`:

```
admin-https-pki-required: disable
admin-lockout-duration: 60
admin-lockout-threshold: 3
admin-maintainer : enable
admintimeout : 5
adom-mode : normal
adom-rev-auto-delete: disable
adom-status : enable
auto-register-device: enable
clt-cert-req : disable
console-output : standard
daylightsavetime : enable
default-disk-quota : 1000
enc-algorithm : low
faz-status : enable
hostname : FMG-VM64-HV
language : english
ldapconntimeout : 60000
log-checksum : none
max-concurrent-users: 20
max-running-reports : 1
partial-install : disable
pre-login-banner : disable
remoteauthtimeout : 10
search-all-adoms : disable
ssl-low-encryption : enable
ssl-protocol : tlsv1 sslv3
task-list-size : 2000
timezone : (GMT-8:00) Pacific Time (US & Canada).
unregister-pop-up : enable
vdom-mirror : disable
webservice-proto : tlsv1
workspace-mode : disabled
```

system ha

Use this command to view HA configuration.

Syntax

```
get system ha
```

Example

This example shows the output for `get system ha`:

```
clusterid : 1
hb-interval : 5
```

```
hb-lost-threshold : 3
mode : standalone
password : *
peer:
```

system interface

Use this command to view interface configuration.

Syntax

```
get system interface
```

Example

This example shows the output for `get system interface`:

```
== [ port1 ]
name: port1 status: up ip: 10.2.115.82 255.255.0.0 speed: auto
== [ port2 ]
name: port2 status: up ip: 0.0.0.0 0.0.0.0 speed: auto
== [ port3 ]
name: port3 status: up ip: 0.0.0.0 0.0.0.0 speed: auto
== [ port4 ]
name: port4 status: up ip: 1.1.1.1 255.255.255.255 speed: auto
```

This example shows the output for `get system interface port1`:

```
name : port1
status : up
ip : 172.16.81.70 255.255.255.0
allowaccess : ping https ssh snmp telnet http
speed : auto
description : (null)
alias : (null)
ipv6:
  ip6-address: ::/0 ip6-allowaccess:
```

system locallog

Use these commands to view local log configuration.

Syntax

```
get system locallog disk filter
get system locallog disk setting
get system locallog fortianalyzer filter
get system locallog fortianalyzer setting
get system locallog memory filter
get system locallog memory setting
get system locallog [syslogd | syslogd2 | syslogd3] filter
get system locallog [syslogd | syslogd2 | syslogd3] setting
```

Example

This example shows the output for `get system locallog disk setting`:

```
status : enable
severity : debug
upload : disable
server-type : FTP
max-log-file-size : 100
roll-schedule : none
diskfull : overwrite
log-disk-full-percentage: 80
```

system log

Use these commands to view log configuration.

Syntax

```
get system log alert
get system log fortianalyzer
get system log settings
```

Example

This example shows the output for `get system log settings`:

```
FAZ-custom-field1 : (null)
FCH-custom-field1 : (null)
FCT-custom-field1 : (null)
FGT-custom-field1 : (null)
FML-custom-field1 : (null)
FWB-custom-field1 : (null)
rolling-regular:
```

system mail

Use this command to view alert email configuration.

Syntax

```
get system mail <server name>
```

system metadata

Use this command to view metadata configuration.

Syntax

```
get system metadata <admin name>
```

system ntp

Use this command to view NTP configuration.

Syntax

```
get system ntp
```

system password-policy

Use this command to view the password policy setting on your device.

Syntax

```
get system password-policy
```

Example

This example shows the output for `get system password-policy`:

```
status : enable
minimum-length : 11
must-contain : upper-case-letter lower-case-letter number non-alphanumeric
change-4-characters : disable
expire : 30
```

system performance

Use this command to view performance statistics on your device.

Syntax

```
get system performance
```

Example

This example shows the output for `get system performance`:

```
CPU:
Used: 2.2%
Used(Excluded NICE): 1.6%
CPU_num: 1.
CPU[0] usage: 4.72%
Usage: %user %nice %sys %idle %iowait %irq %softirq
1.18 1.77 0.79 95.28 0.98 0.00 0.00
Memory:
Total: 4,136,736 KB
Used: 608,908 KB 14.7%
Hard Disk:
Total: 61,923,324 KB
Used: 2,965,900 KB 4.8%
```



```
Flash Disk:
Total: 253,871 KB
Used: 46,426 KB 18.3%
```

system report

Use this command to view report configuration.

Syntax

```
get system report auto-cache
get system report est-browse-time
get system report setting
```

Example

This example shows the output for `get system report auto-cache`:

```
aggressive-drilldown: disable
drilldown-interval : 168
status : enable
```

system route

Use this command to view IPv4 routing table configuration.

Syntax

```
get system route <entry number>
```

system route6

Use this command to view IPv6 routing table configuration.

Syntax

```
get system route6 <entry number>
```

system snmp

Use these commands to view SNMP configuration.

Syntax

```
get system snmp community <community ID>
get system snmp sysinfo
get system snmp user <SNMP user name>
```

Example

This example shows the output for `get system snmp sysinfo`:

```
contact_info : (null)
description : (null)
engine-id : (null)
location : (null)
status : disable
trap-cpu-high-exclude-nice-threshold: 80
trap-high-cpu-threshold: 80
trap-low-memory-threshold: 80
```

system sql

Use this command to view SQL configuration.

Syntax

```
get system sql
```

Example

This example shows the output for `get system sql`:

```
custom-index:
prompt-sql-upgrade : enable
status : local
text-search-index : disable
ts-index-field:
  == [ FGT-app-ctrl ]
  category: FGT-app-ctrl value:
    user,group,srcip,dstip,dstport,service,app,action,status,hostname
  == [ FGT-attack ]
  category: FGT-attack value: severity,srcip,dstip,status,user,attackname
  == [ FGT-content ]
  category: FGT-content value: from,to,subject,action,srcip,dstip,hostname,status
  == [ FGT-dlp ]
  category: FGT-dlp value: user,srcip,service,action,file
  == [ FGT-emailfilter ]
  category: FGT-emailfilter value: user,srcip,from,to,subject
  == [ FGT-event ]
  category: FGT-event value: subtype,ui,action,msg
  == [ FGT-traffic ]
  category: FGT-traffic value: user,srcip,dstip,service,app,utmaction,utmevent
  == [ FGT-virus ]
  category: FGT-virus value: service,srcip,dstip,service,status,file,virus,user
  == [ FGT-voip ]
  category: FGT-voip value: action,user,src,dst,from,to
  == [ FGT-webfilter ]
  category: FGT-webfilter value: user,srcip,dstip,service,status,catdesc,hostname
  == [ FGT-netscan ]
  category: FGT-netscan value: user,dstip,vuln,severity,os
  == [ FML-emailfilter ]
  category: FML-emailfilter value: client_name,dst_ip,from,to,subject
  == [ FML-event ]
```

```

category: FML-event value: subtype,msg
== [ FML-history ]
category: FML-history value: classifier,disposition,from,to,client_
      name,direction,domain,virus
== [ FML-virus ]
category: FML-virus value: src,msg,from,to
== [ FWB-attack ]
category: FWB-attack value: http_host,http_url,src,dst,msg,action
== [ FWB-event ]
category: FWB-event value: ui,action,msg
== [ FWB-traffic ]
category: FWB-traffic value: src,dst,service,http_method,msg
auto-table-upgrade : disable
database-type : postgres
logtype : app-ctrl attack content dlp emailfilter event generic history traffic virus
      voip webfilter netscan
rebuild-event : enable
rebuild-event-start-time: 00:00 1992/01/01
start-time : 23:49 2014/03/14

```

system status

Use this command to view the status of your device.

Syntax

```
get system status
```

Example

This example shows the output for `get system status`:

```

Platform Type : FMG-VM64-HV
Platform Full Name : FortiManager-VM64-HV
Version : v5.0.0-build0345 141020
Serial Number : FMG-VM0A11000XXX
BIOS version : 04000002
Hostname : FMG-VM64-HV
Max Number of Admin Domains : 1120
Max Number of Device Groups : 1120
Admin Domain Configuration : Enabled
HA Mode : Stand Alone
Branch Point : 345
Release Version Information : Interim
Current Time : Tue Oct 21 14:40:13 PDT 2014
Daylight Time Saving : Yes
Time Zone : (GMT-8:00) Pacific Time (US & Canada).
64-bit Applications : Yes
Disk Usage : Free 31.16GB, Total 78.74GB
License Status : Valid

```

system syslog

Use this command to view syslog information.

Syntax

```
get system syslog <syslog server name>
```

show

The `show` commands display a part of your Fortinet unit's configuration in the form of commands that are required to achieve that configuration from the firmware's default state.



Although not explicitly shown in this section, for all `config` commands, there are related `show` commands that display that part of the configuration. The `show` commands use the same syntax as their related `config` command.



CLI commands and variables are case sensitive.

Unlike the `get` command, `show` does not display settings that are assumed to remain in their default state.



Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.